

2.0 Introduction

2.0.1 Why should I take this module?

Welcome to Basic Switch and End Device Configuration!

As part of your career in networking, you might have to set up a new network or maintain and upgrade an existing one. In either case, you'll configure switches and end devices so that they are secure and perform effectively based on your requirements.

Out of the box, switches and end devices come with some general configuration. But for your particular network, switches and end devices require your specific information and instructions. In this module, you will learn how to access Cisco IOS network devices. You will learn basic configuration commands and use them to configure and verify a Cisco IOS device and an end device with an IP address.

Of course, there is much more to network administration, but none of that can happen without first configuring switches and end devices. Let's get started!

2.0.2 What will I learn to do in this module?

Module Title: Basic Switch and End Device Configuration

Module Objective: Implement initial settings including passwords, IP addressing, and default gateway parameters on a network switch and end devices.

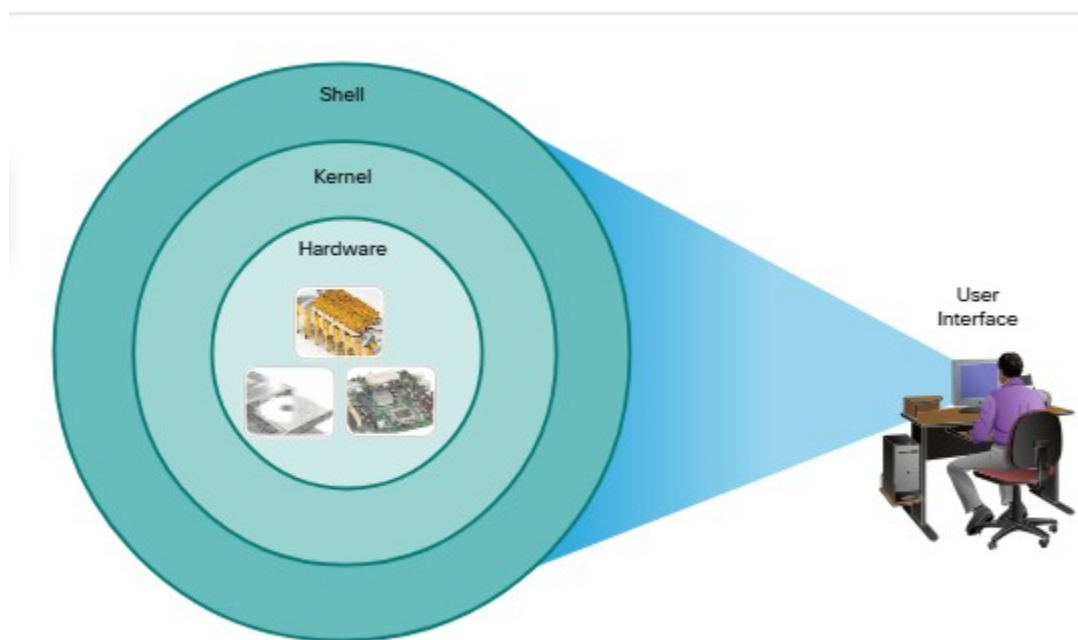
Topic Title	Topic Objective
Cisco IOS Access	Explain how to access a Cisco IOS device for configuration purposes.
IOS Navigation	Explain how to navigate Cisco IOS to configure network devices.
The Command Structure	Describe the command structure of Cisco IOS software.

Basic Device Configuration	Configure a Cisco IOS device using CLI.
Save Configurations	Use IOS commands to save the running configuration.
Ports and Addresses	Explain how devices communicate across network media.
Configure IP Addressing	Configure a host device with an IP address.
Verify Connectivity	Verify connectivity between two end devices.

2.1 Cisco IOS Access

2.1.1 Operating Systems

All end devices and network devices require an operating system (OS). As shown in the figure, the portion of the OS that interacts directly with computer hardware is known as the kernel. The portion that interfaces with applications and the user is known as the shell. The user can interact with the shell using a command-line interface (CLI) or a graphical user interface (GUI).



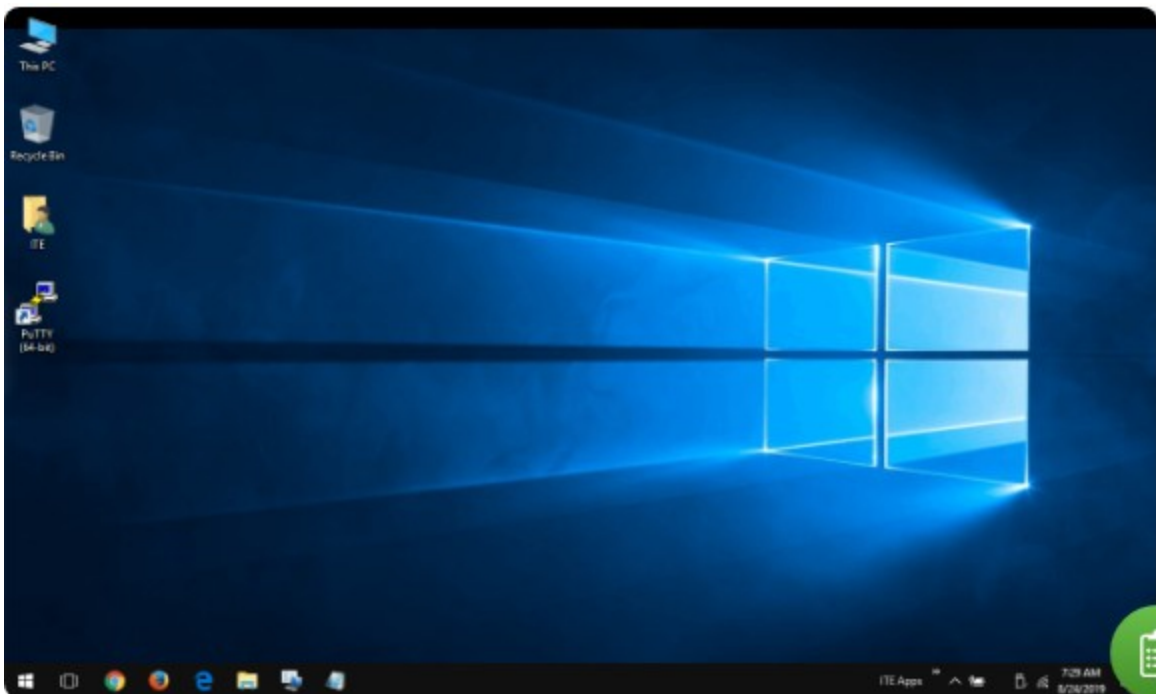
- **Shell** - The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.
- **Kernel** - Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.
- **Hardware** - The physical part of a computer including underlying electronics.

When using a CLI, the user interacts directly with the system in a text-based environment by entering commands on the keyboard at a command prompt, as shown in the example. The system executes the command, often providing textual output. The CLI requires very little overhead to operate. However, it does require that the user have knowledge of the underlying command structure that controls the system.

```
analyst@secOps ~]$ ls
Desktop  Downloads  lab.support.files  second_drive
[analyst@secOps ~]$
```

2.1.2 GUI

A GUI such as Windows, macOS, Linux KDE, Apple iOS, or Android allows the user to interact with the system using an environment of graphical icons, menus, and windows. The GUI example in the figure is more user-friendly and requires less knowledge of the underlying command structure that controls the system. For this reason, most users rely on GUI environments.



However, GUIs may not always be able to provide all the features available with the CLI. GUIs can also fail, crash, or simply not operate as specified. For these reasons, network devices are typically accessed through a CLI. The CLI is less resource intensive and very stable when compared to a GUI.

The family of network operating systems used on many Cisco devices is called the Cisco Internetwork Operating System (IOS). Cisco IOS is used on many Cisco routers and switches regardless of the type or size of the device. Each device router or switch type uses a different version of Cisco IOS. Other Cisco operating systems include IOS XE, IOS XR, and NX-OS.

Note: The operating system on home routers is usually called firmware. The most common method for configuring a home router is by using a web browser-based GUI.

2.1.3 Purpose of an OS

Network operating systems are similar to a PC operating system. Through a GUI, a PC operating system enables a user to do the following:

- Use a mouse to make selections and run programs

- Enter text and text-based commands

- View output on a monitor

A CLI-based network operating system (e.g., the Cisco IOS on a switch or router) enables a network technician to do the following:

- Use a keyboard to run CLI-based network programs

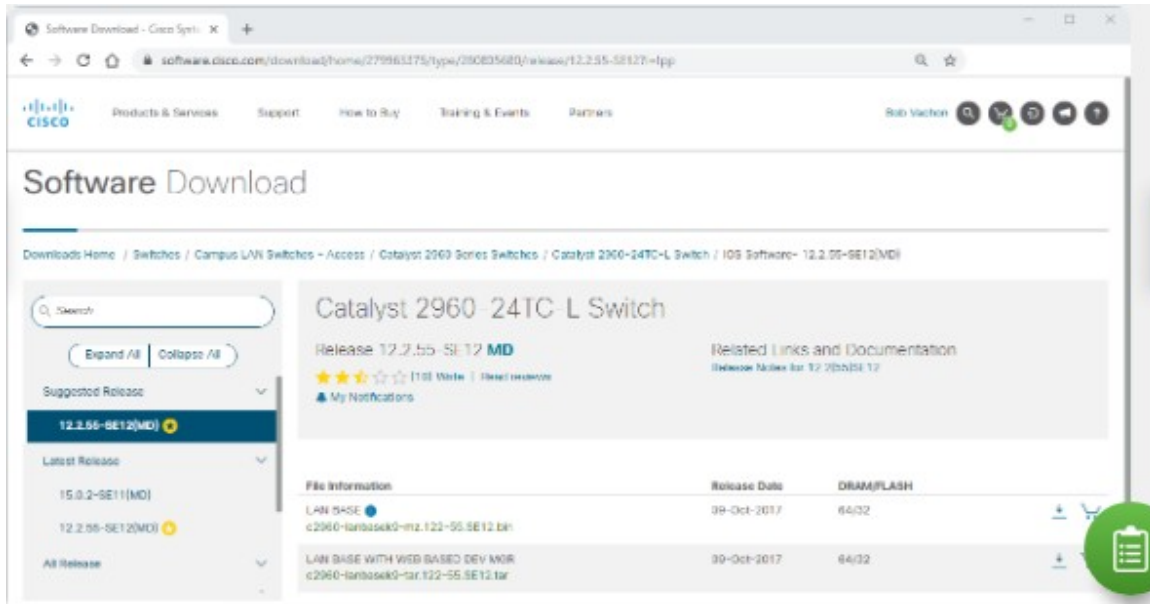
- Use a keyboard to enter text and text-based commands

- View output on a monitor

Cisco networking devices run particular versions of the Cisco IOS. The IOS version is dependent on the type of device being used and the required features. While all devices come with a default IOS and feature set, it is possible to upgrade the IOS version or feature set to obtain additional capabilities.

The figure displays a list of IOS software releases for a Cisco Catalyst 2960 Switch.

Cisco Software Download Example



2.1.4 Access Methods

A switch will forward traffic by default and does not need to be explicitly configured to operate. For example, two configured hosts connected to the same new switch would be able to communicate.

Regardless of the default behavior of a new switch, all switches should be configured and secured.

Method	Description
--------	-------------

Console	This is a physical management port that provides out-of-band access to a Cisco device. Out-of-band access refers to access via a dedicated management that is used for device maintenance purposes only. The advantage of using a console port is that the device is accessible even if no networking services are configured, such as performing the initial configuration. A computer running terminal emulation software and a special console cable to connect to the device are required for a console connection.
---------	---

Secure Shell (SSH) SSH is an in-band and recommended method for remotely establishing a secure CLI connection, through a virtual interface, over a network. Unlike a console connection, SSH connections require active networking services on the device, including an active interface configured with an address. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.

Telnet Telnet is an insecure, in-band method of remotely establishing a CLI session, through a virtual interface, over a network. Unlike SSH, Telnet does not provide a secure, encrypted connection and should only be used in a lab environment. User authentication, passwords, and commands are sent over the network in plaintext. The best practice is to use SSH instead of Telnet. Cisco IOS includes both a Telnet server and a Telnet client.

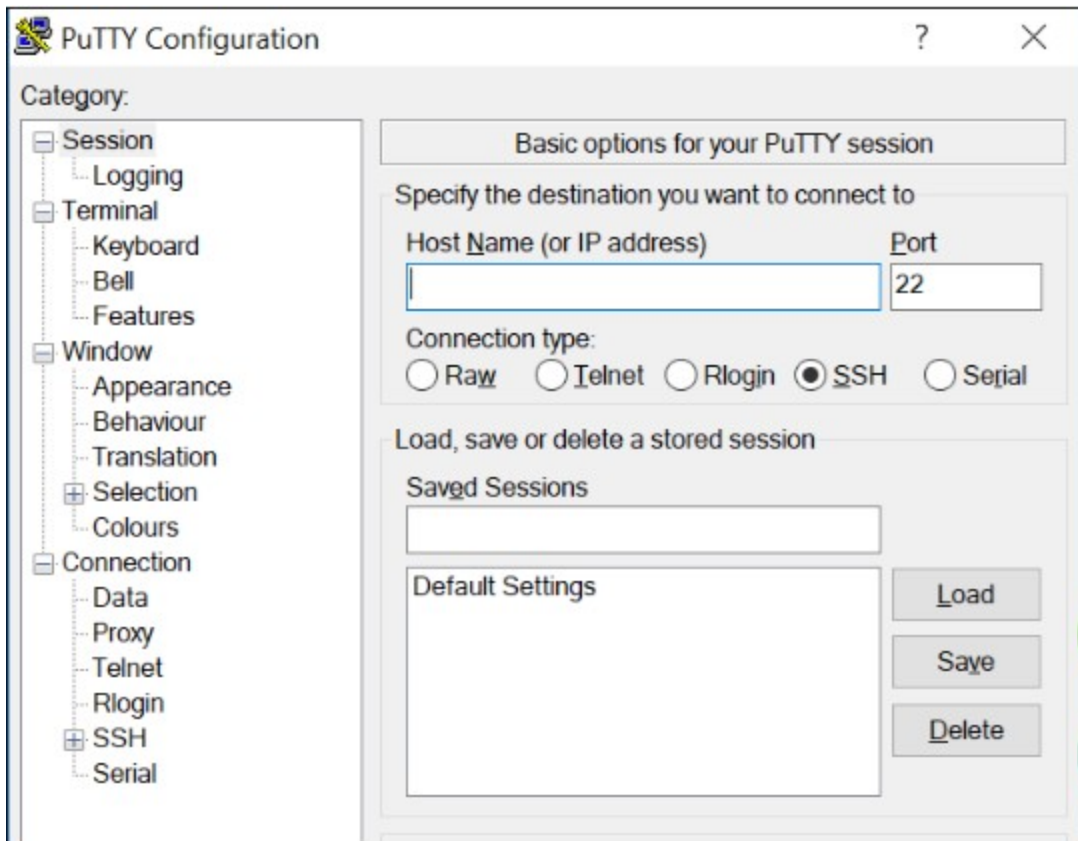
Note: Some devices, such as routers, may also support a legacy auxiliary port that was used to establish a CLI session remotely over a telephone connection using a modem. Similar to a console connection, the AUX port is out-of-band and does not require networking services to be configured or available.

2.1.5 Terminal Emulation Programs

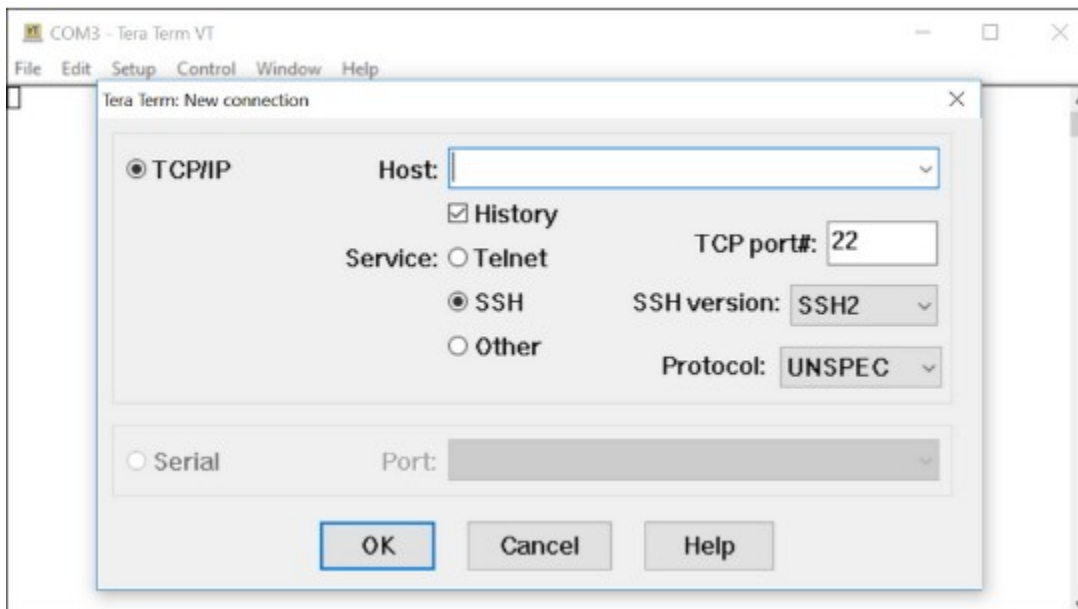
There are several terminal emulation programs you can use to connect to a networking device either by a serial connection over a console port, or by an SSH/Telnet connection. These programs allow you to enhance your productivity by adjusting window sizes, changing font sizes, and changing color schemes.

Click each program name to see a screen capture of the interface.

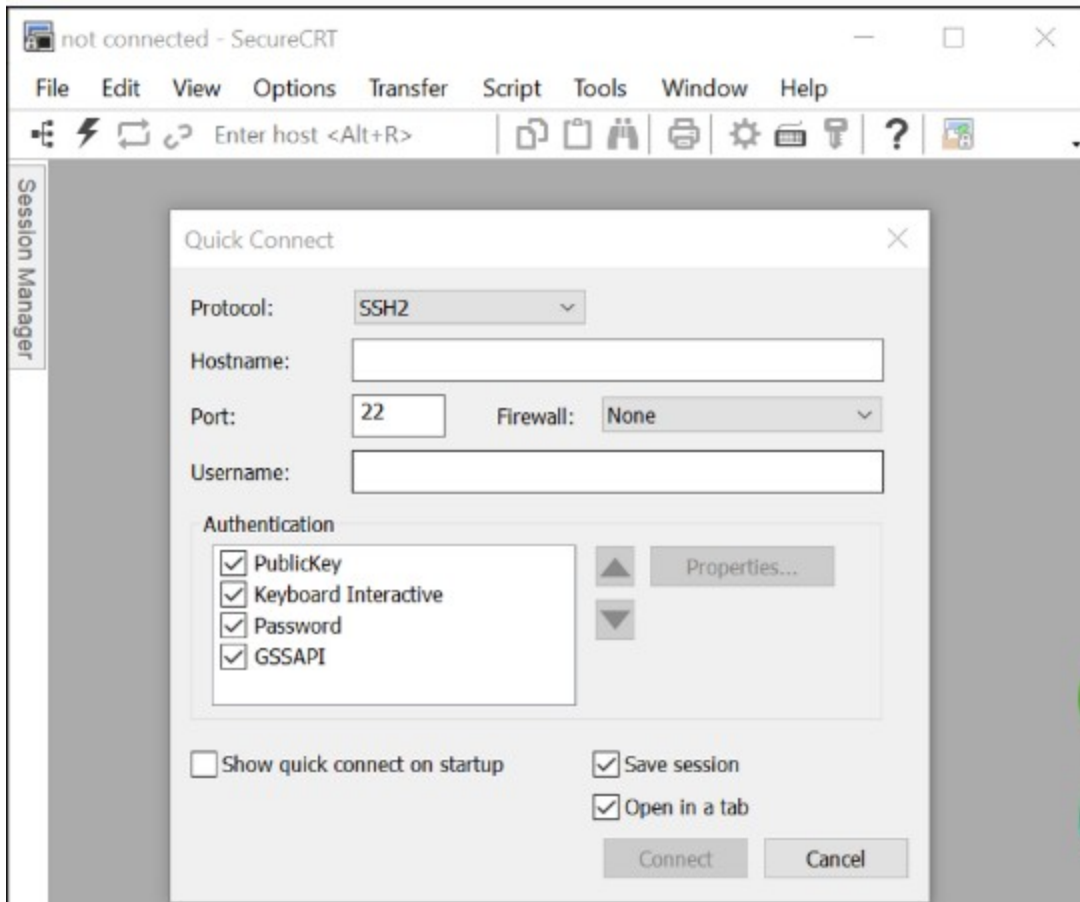
Putty



Tera Term



SecureCRT



2.1.6 Check Your Understanding - Cisco IOS Access

Check your understanding of Cisco IOS Access by choosing the BEST answer to the following questions.

Question 1

Which access method would be most appropriate if you were in the equipment room with a new switch that needs to be configured?

done

Console

Telnet/SSH

Aux

Question 2

Which access method would be most appropriate if your manager gave you a special cable and told you to use it to configure the switch?

done

Console

Telnet/SSH

Aux

Question 3

Which access method would be the most appropriate in-band access to the IOS over a network connection?

Console

done

Telnet/SSH

Aux

Question 4

Which access method would be the most appropriate if you call your manager to tell him you cannot access your router in another city over the internet and he provides you with the information to access the router through a telephone connection?

Console

Telnet/SSH

done

Aux

100%

You've scored 100%.

Congratulations, you have passed the quiz!

You've submitted your answers!

Reset

2.2 IOS Navigation

2.2.1 Primary Command Modes

In the previous topic, you learned that all network devices require an OS and that they can be configured using the CLI or a GUI. Using the CLI may provide the network administrator with more precise control and flexibility than using the GUI. This topic discusses using CLI to navigate the Cisco IOS.

As a security feature, the Cisco IOS software separates management access into the following two command modes:

User EXEC Mode - This mode has limited capabilities but is useful for basic operations. It allows only a limited number of basic monitoring commands but does not allow the execution of any commands that might change the configuration of the device. The user EXEC mode is identified by the CLI prompt that ends with the > symbol.

Privileged EXEC Mode - To execute configuration commands, a network administrator must access privileged EXEC mode. Higher configuration modes, like global configuration mode, can only be reached from privileged EXEC mode. The privileged EXEC mode can be identified by the prompt ending with the # symbol.

The table summarizes the two modes and displays the default CLI prompts of a Cisco switch and router.

Command Mode	Description	Default Device Prompt
User Exec Mode	• Mode allows access to only a limited number of basic monitoring commands. • It is often referred to as "view-only" mode.	Switch> Router>
Privileged EXEC Mode	• Mode allows access to all commands and features. • The user can use any monitoring commands and execute configuration and management commands.	Switch# Router#

2.2.2 Configuration Mode and Subconfiguration Modes

To configure the device, the user must enter global configuration mode, which is commonly called global config mode.

From global config mode, CLI configuration changes are made that affect the operation of the device as a whole. Global configuration mode is identified by a prompt that ends with (config)# after the device name, such as Switch(config)#.

Global configuration mode is accessed before other specific configuration modes. From global config mode, the user can enter different subconfiguration modes. Each of these modes allows the configuration of a particular part or function of the IOS device. Two common subconfiguration modes include:

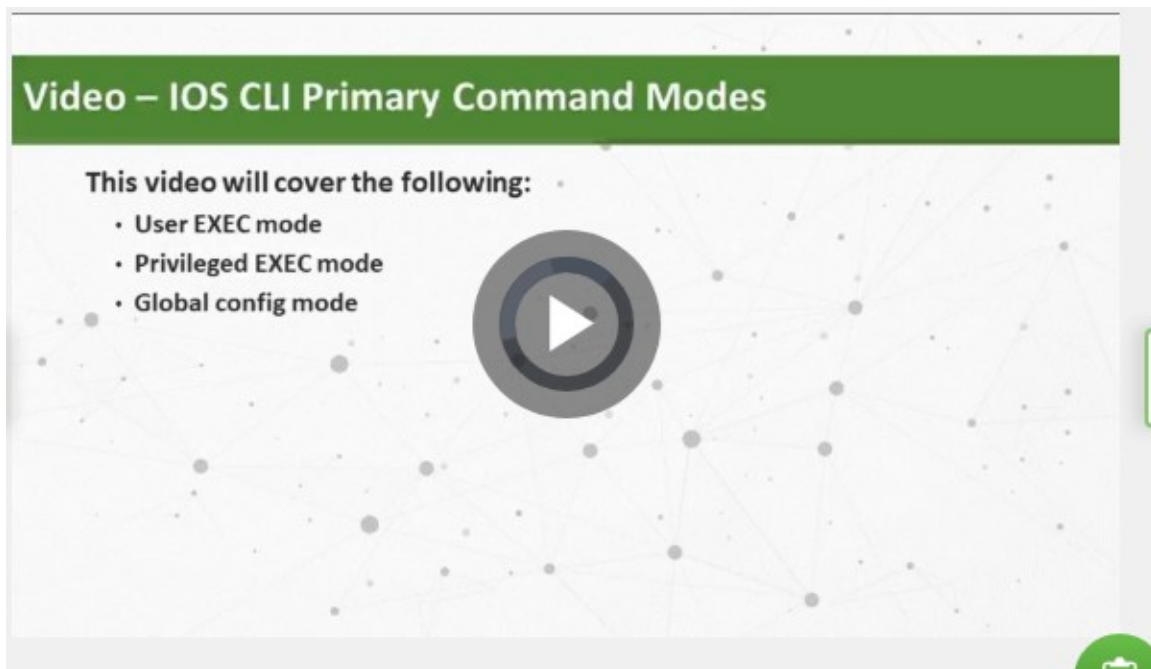
Line Configuration Mode - Used to configure console, SSH, Telnet, or AUX access.

Interface Configuration Mode - Used to configure a switch port or router network interface.

When the CLI is used, the mode is identified by the command-line prompt that is unique to that mode. By default, every prompt begins with the device name. Following the name, the remainder of the prompt indicates the mode. For example, the default prompt for line configuration mode is **Switch(config-line)#** and the default prompt for interface configuration mode is **Switch(config-if)#**.

2.2.3 Video - IOS CLI Primary Command Modes

Click Play in the figure to view a video demonstration of navigating between IOS modes.



Transcript

Follow along using the transcript.

Show

Transcript

Transcript

16px (

default

)

English

00:04

[Speaker] Lets examine the Cisco IOS command modes,

00:07

I'll click on PC1,

00:09

click on the Terminal emulation program,

00:12

click okay, and you can see that I'm presented

00:15

with a console command line interface.

00:18

This is the Cisco IOS.

00:21

I'll press enter on my keyboard to get started,

00:23

notice the command prompt at the bottom left

00:26

of the screen. Which indicates the command mode,

00:29

that I am in.

00:30

The Cisco IOS uses different command modes

00:32

to establish various privilege levels for users.

00:36

Different commands are available in each mode.

00:39

For instance the word switch, which is

00:42

the default name of the switch

00:44

with the greater than sign indicates,

00:46

that I am in user accept mode.

00:49

User accept mode has very little privileges

00:51

with access to only a limited number of commands.

00:55

One of those commands available in this mode,

00:57

is the Enable Command.

01:00

At the blinking cursor I'll type the command enable

01:03

and press enter, and I am now in

01:05

Privileged EXEC mode.

01:08

I can tell this because the prompt has changed

01:10

from a greater than sign

01:12

to a hash or a pound sign.

01:16

Privileged EXEC mode offers a higher

01:18

privileged level for the user and

01:21

more commands are available.

01:23

If I would like to go to a higher level,

01:25

I can go into global configuration mode

01:28

or global config mode for short.

01:31

I can reach global config mode,

01:33

by typing in configure terminal

01:36

and pressing enter,

01:38

and now you can see

01:40

the global configuration prompt.

01:42

This is where most configurations of a

01:45

switch or a router take place.

01:47

There are also some configuration modes

01:50

like interface configuration mode,

01:52

if I type interface vlan 1 and press enter.

01:57

I'm presented with a prompt that indicates

02:00

I am now in interface configuration mode.

02:05

Many commands will only work

02:07

from within certain modes

02:09

a common mistake made by users

02:11

new to working with a Cisco IOS

02:13

is trying to use commands from within

02:16

the wrong mode.

02:17

If you are sure that you are typing

02:19

a command correctly, but you

02:21

are continuously getting an error message

02:24

always check your prompt,

02:25

to make sure you are in the right

02:27

mode.

2.2.4 Navigate Between IOS Modes

Various commands are used to move in and out of command prompts. To move from user EXEC mode to privileged EXEC mode, use the enable command. Use the disable privileged EXEC mode command to return to user EXEC mode.

Note: Privileged EXEC mode is sometimes called enable mode.

To move in and out of global configuration mode, use the configure terminal privileged EXEC mode command. To return to the privileged EXEC mode, enter the exit global config mode command.

There are many different subconfiguration modes. For example, to enter line subconfiguration mode, you use the line command followed by the management line type and number you wish to access. Use the exit command to exit a subconfiguration mode and return to global configuration mode.

```
Switch(config)# line console 0
Switch(config-line)# exit
Switch(config)#
```

To move from any subconfiguration mode of the global configuration mode to the mode one step above it in the hierarchy of modes, enter the **exit** command.

To move from any subconfiguration mode to the privileged EXEC mode, enter the **end** command or enter the key combination **Ctrl+Z**.

```
Switch(config-line)# end
Switch#
```

You can also move directly from one subconfiguration mode to another. Notice how after selecting an interface, the command prompt changes from **(config-line)#** to **(config-if)#**.

```
Switch(config-line)# interface FastEthernet 0/1
Switch(config-if)#
```

2.2.5 Video - Navigate Between IOS Modes

Click Play in the figure to view a video demonstration of how to move between various IOS CLI modes.

Video – Navigate between IOS Modes

This video will cover the following:

- enable
- disable
- configure terminal
- exit
- end
- Control + Z on keyboard
- Other commands to enter sub configuration modes



Transcript

Follow along using the transcript.

 Show Transcript



Transcript

16px (
default
)

English

00:04

- [Instructor] Let's look at the commands that are used

00:05

to move between the different iOS command modes.

00:08

We'll look at the enable command, the disable command,

00:13

configure terminal, exit and using Ctrl+Z on your keyboard,

00:19

plus some commands to enter different

00:21

sub-configuration modes.

00:23

I have a console connection to a switch,

00:25

so I'll click on PC one, and press Enter.

00:30

And it takes me to User EXEC mode.

00:32

Notice the prompt at the lower left of the screen.

00:36

To enter Privileged EXEC mode, I type enable.

00:40

If I want to return back to User EXEC mode,

00:43

I can type disable.

00:46

I'll type enable to return to Privileged EXEC mode.

00:49

In order to configure the switch, I need to first

00:53

get to Global Configuration mode or Global Config.

00:56

I'll type configure terminal.

01:01

And you can see now

01:02

that I'm in the Global Configuration prompt.

01:05

I can type exit and press Enter

01:09

to return to Privileged EXEC mode.

01:12

If I type exit again,

01:14

I'll leave my console connection all together.

01:17

To re-enter the switch and get a Command Line Interface,

01:20

I have to press Enter on my keyboard,

01:23

and now I'm brought back

01:24

to the console connection with the switch.

01:26

I'll type enable, and press Enter,

01:29

and then config t short for configure terminal,

01:32

and now I'm back in Global Config mode.

01:35

Let's enter one of the sub-configuration modes.

01:38

I'll type line console zero

01:42

to get to the management interface for the console port.

01:46

Now that I'm in a sub-configuration mode, if I type exit,

01:50

I returned to Global Config mode.

01:53

This time I'll type line vty zero space 15,

01:59

for my Virtual Terminal Management interfaces.

02:02

These are used for remote administrative access

02:04

to the switch.

02:05

I can move directly

02:06

from one sub-configuration mode to another.

02:09

Notice if I type in

02:12

interface vlan one and press Enter,

02:16

that my prompt has changed from Line Configuration mode

02:20

to Interface Configuration mode.

02:23

From here, I can also enter different interfaces,

02:26

like interface fastethernet

02:33

zero slash one,

02:35

and as long as I don't see an error message

02:37

that I've typed in invalid command,

02:39

I'm in Interface Config mode for fastethernet 01.

02:43

I can also move directly to the line console zero.

02:48

Commands that are normally run in Global Config mode

02:50

can also be run

02:51

from any of the sub-configuration modes as well.

02:54

If I want to exit out of all sub-configuration modes

02:58

and return to Privileged EXEC mode,

03:01

I can use the end command or press Ctrl+Z on my keyboard.

03:06

Let's give that a try.

03:07

I'll type end, press Enter+Enter again.

03:10

And you can see now that I've returned

03:12

all the way back to Privileged EXEC mode.

03:15

I'll return to Global Configuration mode.

03:18

And then into line console zero.

03:22

And this time, I'll hold down the Ctrl key and press z.

03:27

And if I press Enter, you can see that I'm brought

03:30

all the way back to Privileged EXEC mode.

03:33

If I'm in Global Configuration mode,

03:36

and I type end, and press Enter,

03:39

I'm also brought back to Privileged EXEC mode.

03:42

Learning to navigate efficiently between

03:45

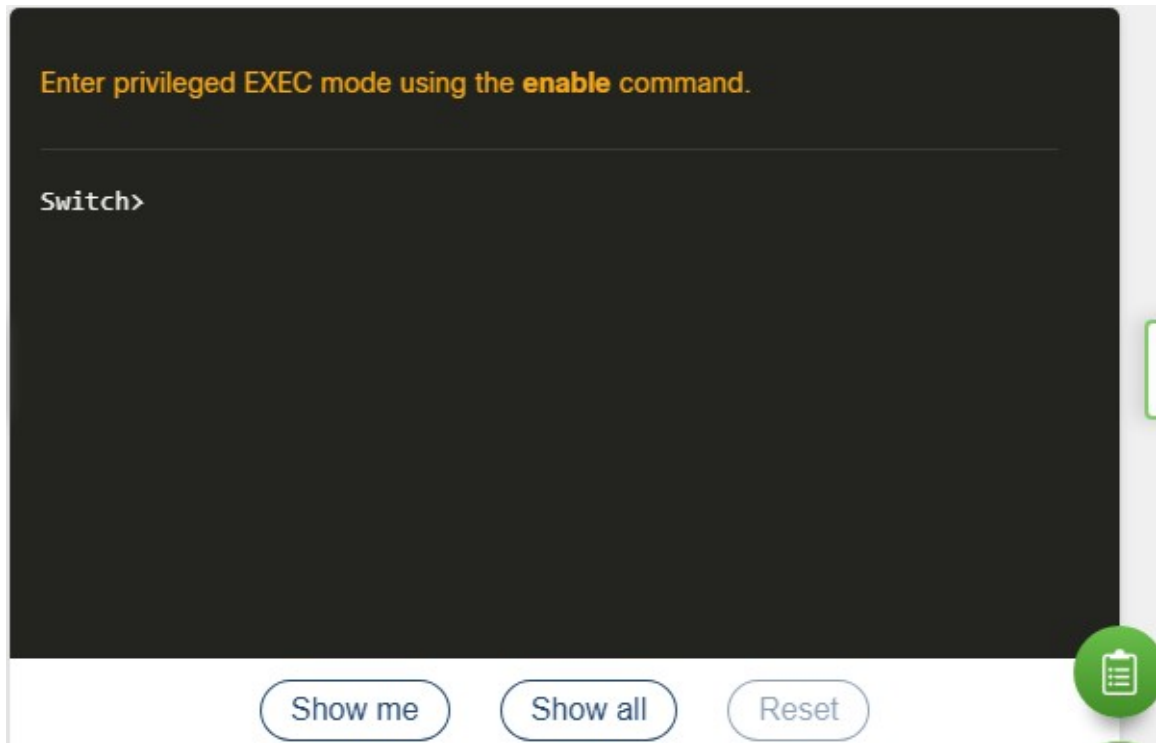
the different command modes will save you a lot of time.

2.2.6 A Note About Syntax Checker Activities

When you are learning how to modify device configurations, you might want to start in a safe, non-production environment before trying it on real equipment. NetAcad gives you different simulation tools to help build your configuration and troubleshooting skills. Because these are simulation tools, they typically do not have all the functionality of real equipment. One such tool is the Syntax Checker. In each Syntax Checker, you are given a set of instructions to enter a specific set of commands. You cannot progress in Syntax Checker unless the exact and full command is entered as specified. More advanced simulation tools, such as Packet Tracer, let you enter abbreviated commands, much as you would do on real equipment.

2.2.7 Syntax Checker - Navigate Between IOS Modes

Use the Syntax Checker activity to navigate between IOS command lines on a switch.



Enter privileged EXEC mode using the enable command.

```
Switch>enable
```

Return to user EXEC mode using the disable command.

```
Switch#disable
```

Re-enter privileged EXEC mode.

```
Switch>enable
```

Enter global configuration mode using the configure terminal command.

```
Switch#configure terminal
```

Exit global configuration mode and return to privileged EXEC mode using the exit command.

Switch(config)#exit

Re-enter global configuration mode.

Switch#configure terminal

Enter line subconfiguration mode for the console port using the line console 0 command.

Switch(config)#line console 0

Return to global configuration mode using the exit command.

Switch(config-line)#exit

Enter VTY line subconfiguration mode using the line vty 0 15 command.

Switch(config)#line vty 0 15

Return to global configuration mode.

Switch(config-line)#exit

Enter the VLAN 1 interface subconfiguration mode using the interface vlan 1 command.

Switch(config)#interface vlan 1

From interface configuration mode, switch to line console subconfiguration mode using the line console 0 global configuration command.

Switch(config-if)#line console 0

Return to privileged EXEC mode using the end command.

Switch(config-line)#end

You successfully navigated between the various IOS command line modes.

2.2.8 Check Your Understanding - IOS Navigation

Check your understanding of IOS navigation by choosing the correct answer to the following questions.

Question 1

Which IOS mode allows access to all commands and features?

Global configuration mode

Interface subconfiguration mode

Line console subconfiguration mode

done

Privileged EXEC mode

User EXEC mode

Question 2

Which IOS mode are you in if the Switch(config)# prompt is displayed?

done

Global configuration mode

Interface subconfiguration mode

Line console subconfiguration mode

Privileged EXEC mode

User EXEC mode

Question 3

Which IOS mode are you in if the Switch> prompt is displayed?

Global configuration mode

Interface subconfiguration mode

Line console subconfiguration mode

Privileged EXEC mode

done

User EXEC mode

Question 4

Which two commands would return you to the privileged EXEC prompt regardless of the configuration mode you are in? (Choose two.)

done

CTRL+Z

disable

enable

done

end

exit

100%

You've scored 100%.

Congratulations, you have passed the quiz!

You've submitted your answers!

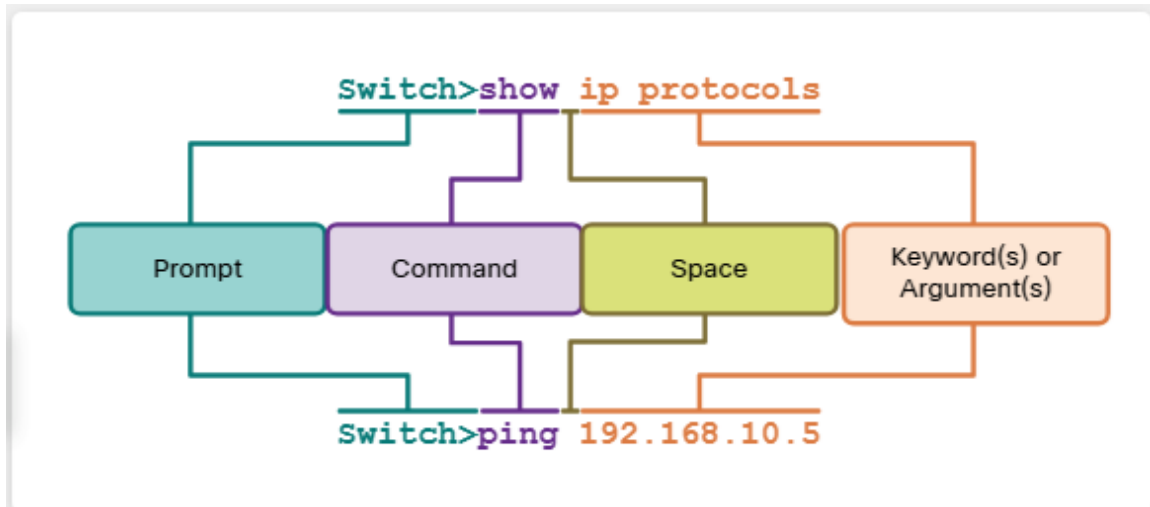
Reset

2.3 The Command Structure

2.3.1 Basic IOS Command Structure

This topic covers the basic structure of commands for the Cisco IOS. A network administrator must know the basic IOS command structure to be able to use the CLI for device configuration.

A Cisco IOS device supports many commands. Each IOS command has a specific format, or syntax, and can only be executed in the appropriate mode. The general syntax for a command, shown in the figure, is the command followed by any appropriate keywords and arguments.



- **Keyword** - This is a specific parameter defined in the operating system (in the figure, **ip protocols**).
- **Argument** - This is not predefined; it is a value or variable defined by the user (in the figure, **192.168.10.5**).

After entering each complete command, including any keywords and arguments, press the **Enter** key to submit the command to the command interpreter.

2.3.2 IOS Command Syntax Check

A command might require one or more arguments. To determine the keywords and arguments required for a command, refer to the command syntax. The syntax provides the pattern, or format, that must be used when entering a command.

As identified in the table, boldface text indicates commands and keywords that are entered as shown. Italic text indicates an argument for which the user provides the value.

Convention Description

boldface Boldface text indicates commands and keywords that you enter literally as shown.

italics Italic text indicates arguments for which you supply values.

[x] square brackets indicate an optional element (keyword or argument).

{x} Braces indicate a required element (keyword or argument).

[x{y | z }] Braces and vertical lines within square brackets indicate a required choice within an optional element. Spaces are used to clearly delineate parts of the command.

For instance, the syntax for using the description command is `description string`. The argument is a string value provided by the user. The description command is typically used to identify the purpose of an interface. For example, entering the command, `description Connects to the main headquarter office switch`, describes where the other device is at the end of the connection.

The following examples demonstrate conventions used to document and use IOS commands:

ping *ip-address* - The command is `ping` and the user-defined argument is the *ip-address* of the destination device. For example, **ping 10.10.10.5**.

traceroute *ip-address* - The command is `traceroute` and the user-defined argument is the *ip-address* of the destination device. For example, **traceroute 192.168.254.254**.

If a command is complex with multiple arguments, you may see it represented like this:

```
Switch(config-if)# switchport port-security aging { static  
| time time | type {absolute | inactivity}
```

The command will typically be followed with a detailed description of the command and each argument.

The Cisco IOS Command Reference is the ultimate source of information for a particular IOS command.

2.3.3 IOS Help Features

The IOS has two forms of help available: context-sensitive help and command syntax check.

Context-sensitive help enables you to quickly find answers to these questions:

Which commands are available in each command mode?

Which commands start with specific characters or group of characters?

Which arguments and keywords are available to particular commands?

To access context-sensitive help, simply enter a question mark, **?**, at the CLI.

Command syntax check verifies that a valid command was entered by the user. When a command is entered, the command line interpreter evaluates the command from left to right. If the interpreter understands the command, the requested action is executed, and the CLI returns to the appropriate prompt. However, if the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

2.3.4 Video - Context Sensitive Help and Command Syntax Check

Click Play in the figure to view a video demonstration of context-sensitive help and command syntax check.

Video - Context-Sensitive Help and Command Syntax Check

This video covers the following:

- Use the help command in user EXEC, privileged EXEC, and global config modes
- Finish commands and arguments with the help command
- Use the command syntax checker to fix syntax errors and incomplete commands

Transcript

Follow along using the transcript.

 Show Transcript

Transcript

16px (
default
)

English

00:01

- The CISCO IOS help command,

00:03

is accessed by using the question mark.

00:06

The help command is context sensitive,

00:08

so it matters how and where you use the question mark.

00:14

For instance, let's say I want a list of all the commands

00:18

that are available to me in user-exec mode.

00:20

I simply type a question mark,

00:22

and I'm returned the commands that are available

00:25

in user-exact mode.

00:27

If I type enable,

00:29

and enter privileged-exec mode,

00:31

and put in a question mark,

00:33

I'm given the commands, that are available to me,

00:35

in privileged-exec mode.

00:37

I'll press the space bar to get the next page of output.

00:41

And even different set of commands

00:42

is available to the user

00:44

in global configuration mode.

00:46

Notice I'll go to global-config mode,

00:48

put in a question mark,

00:49

and then given a completely different set of commands,

00:53

that are available in this particular command mode.

00:56

There are other uses for the help command as well.

01:00

Let's say that I don't want a listing

01:02

of all of the commands that are available,

01:05

and I just want help finishing one particular command.

01:08

For instance, let's say

01:10

I'm putting in the command interface

01:12

but I've forgotten what the complete command name is.

01:15

I've typed I-N and I need help finishing the command.

01:20

I can put in part of the command,

01:22

and then put in a question mark,

01:24

and it'll help me finish the command.

01:26

Notice that I've put in I-N and then a question mark,

01:30

and the help command, has returned,

01:33

that the command that I'm looking for is interface.

01:36

I can use the help command in another context as well.

01:40

So now that I know that the command is interface.

01:44

Let's say I'm not sure what the next command parameter

01:48

or argument is that goes with the interface command.

01:53

In this case I'll put a space and then a question mark,

01:56

and it will tell me, the next parameter or argument,

02:00

that is required by the interface command.

02:03

Now I know that the next part of the command,

02:05

is either the name of the interface

02:08

like Ethernet, FastEthernet, GigabitEthernet,

02:11

or maybe it's Vlan, or range.

02:15

Related to the help command is the command's syntax checker.

02:19

The command's syntax checker

02:20

will let me know when I have a problem

02:23

with the command that I have put in.

02:25

For instance, we can see here

02:27

that the next part of this command

02:29

would be one of these arguments here.

02:32

Let's say I make a mistake and I type in the number 33

02:35

instead of Vlan or range and hit enter.

02:39

Notice that the command syntax checker has informed me

02:43

that beginning at the number three,

02:46

I've made an invalid input.

02:48

This is extremely useful because it helps me

02:51

to isolate where the problem is

02:53

with the particular command that I've entered.

02:56

This can work in different contexts as well.

02:58

For instance, let's say, that I've put in

03:01

just the letter I instead of interface and I hit enter.

03:06

The command syntax checker informs me

03:08

that the letter I is an ambiguous command.

03:12

The reason being is that, if I type in I,

03:15

and a question mark

03:16

there's actually two commands that begin with the letter I

03:19

In global configuration mode.

03:22

The command interface and the command ip.

03:24

The third example of the command syntax checker

03:27

is when I type in interface and hit enter.

03:31

And the command syntax checker has informed me

03:34

that the command is incomplete.

03:36

To solve this, I put in interface again,

03:40

a space and a question mark,

03:42

and I'm given the next set of options

03:45

that I need to finish this command.

03:47

You can see how the help command is very useful

03:51

in learning the different commands that are available to you

03:54

as well as the correct context

03:56

and use of the different commands.

2.3.5 Hot Keys and Shortcuts

The IOS CLI provides hot keys and shortcuts that make configuring, monitoring, and troubleshooting easier.

Commands and keywords can be shortened to the minimum number of characters that identify a unique selection. For example, the configure command can be shortened to conf because configure is the only command that begins with conf. An even shorter version, con, will not work because more than one command begins with con. Keywords can also be shortened.

The table lists keystrokes to enhance command line editing.

Keystroke	Description
Tab	Completes a partial command name entry.
Backspace	Erases the character to the left of the cursor.
Ctrl+D	Erases the character at the cursor.
Ctrl+K	Erases all characters from the cursor to the end of the command line.
Esc D	Erases all characters from the cursor to the end of the word.
Ctrl+U or Ctrl+X	Erases all characters from the cursor back to the beginning of the command line.
Ctrl+W	Erases the word to the left of the cursor.
Ctrl+A	Moves the cursor to the beginning of the line.
Left Arrow or Ctrl+B	Moves the cursor one character to the left

Esc B Moves the cursor back one word to the left.

Esc F Moves the cursor forward one word to the right.

Right Arrow or Ctrl+F Moves the cursor one character to the right.

Ctrl+E Moves the cursor to the end of command line.

Up Arrow or Ctrl+P Recalls the previous command in the history buffer, beginning with the most recent command.

Down Arrow or Ctrl+N Goes to the next line in the history buffer.

Ctrl+R or Ctrl+I or Ctrl+L Redisplays the system prompt and command line after a console message is received.

Note: While the Delete key typically deletes the character to the right of the prompt, the IOS command structure does not recognize the Delete key.

When a command output produces more text than can be displayed in a terminal window, the IOS will display a "--More--" prompt. The following table describes the keystrokes that can be used when this prompt is displayed.

Keystroke	Description
-----------	-------------

Enter key	Displays the next line.
------------------	-------------------------

Space bar	Displays the next screen.
------------------	---------------------------

Any other key *	Ends the display string, returning to previous prompt. *
Except "y", which answers "yes" to the --More-- prompt, and acts like the Space bar.	

This table lists commands used to exit out of an operation.

Keystroke	Description
-----------	-------------

Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode. When in setup mode, aborts back to the command prompt.
--------	---

Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
--------	--

Ctrl-Shift-6	All-purpose break sequence used to abort DNS lookups, traceroutes, pings, etc.
--------------	--

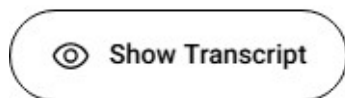
2.3.6 Video - Hot Keys and Shortcuts

Click Play in the figure to view a video demonstration of the various hotkeys and shortcuts.



Transcript

Follow along using the transcript.



Transcript

16px (
default
)

English

00:03

- Support for hot keys and shortcuts makes

00:05

the Cisco IOS extremely efficient.

00:08

Making use of these will save you lots of time

00:11

when you're configuring devices.

00:13

I have a console connection to a switch,

00:15

however, instead of using the terminal emulation program

00:18

to console in, this time I'll click directly

00:21

on the switch and go to the CLI Tab.

00:26

If press Enter,

00:27

I'm taken to the Command Line Interface.

00:30

This is a convenient shortcut to the CLI

00:32

available to you within Packet Tracer.

00:35

The first hot key that I'll talk about

00:37

is the Tab key, or Tab completion,

00:39

for automatically completing your commands.

00:42

You can use it like this.

00:44

To get to Privileged EXEC Mode,

00:46

I would normally type the command Enable.

00:48

With Tab completion, you simply type

00:51

the first few letters of the command,

00:53

in this case E-N,

00:55

and press the Tab key on your keyboard

00:58

and the command is automatically completed for you.

01:01

This is very useful.

01:03

This will work if only one command begins

01:05

with the letters E-N.

01:07

For instance, if I want to put in the command configure

01:11

for configure terminal,

01:12

and I type in C-O-N and press Tab,

01:15

it doesn't work.

01:17

The command isn't completed.

01:19

That's because if I put in a question mark,

01:22

you can see that there's more than one command beginning

01:25

with the letters C-O-N in Privileged EXEC Mode.

01:29

If I want to use Tab completion,

01:31

I'll need to type C-O-N-F

01:34

and press the Tab key.

01:36

You can see that the command is completed.

01:39

For terminal, all I need to do

01:41

is type the letter T

01:43

and press the Tab key as there's only one argument

01:47

or secondary command that follows configure

01:50

and begins with the letter T.

01:52

So the switch knows that the command I want is "terminal."

01:55

Even better than using the Tab key is command shortening.

01:59

With command shortening, instead of pressing the Tab key

02:01

to complete the command,

02:03

you simply use the first few letters of the command

02:06

and the IOS will accept the shortened command

02:08

without hitting the Tab key.

02:10

This is extremely useful.

02:12

For instance, instead of typing the command,

02:15

"interface fast ethernet 0/1"

02:18

which is a very long command to type,

02:20

I can shorten the command to just I-N-T,

02:23

which is short for interface,

02:25

F, short for fast ethernet,

02:28

and "0/1" and press Enter.

02:31

The IOS automatically knows the command I want

02:33

and executes it.

02:35

Though, you won't see it displayed

02:36

as you do with the Tab completion.

02:38

Command shortening can make you

02:40

even more efficient when configuring devices.

02:43

Sometimes it's necessary to repeat commands.

02:46

The fastest way to do this is to cycle

02:48

through your command history using

02:50

your Up Arrow and Down Arrow keys.

02:53

If I type "end" on my keyboard and press Enter,

02:57

to go back to Privileged EXEC Mode,

03:00

and then I press my Up Arrow key,

03:03

you can see that there are two commands

03:05

in my command history.

03:07

Pressing the Down Arrow key will

03:10

take me forwards in my command history.

03:12

This is very useful for commands that are used repeatedly.

03:16

Let's take a look at some hot keys.

03:18

Both Control + Z and Control + C will take use back

03:22

to Privileged EXEC Mode.

03:24

If I hold down Control + Z,

03:27

and press Enter,

03:29

you can see that I'm back to the Privileged EXEC prompt.

03:32

Control + C will do the same

03:34

and it can also be used to abort certain commands.

03:37

For instance, if I type C-O-N-F and T,

03:42

and then change my mind,

03:44

I can press Control + C

03:47

and the command is aborted.

03:49

Control + A will jump the cursor to the beginning of a line.

03:53

I'll type configure

03:56

and then press Control + A

03:58

and you can see that the blinking cursor is now back

04:01

to the beginning of the line.

04:03

If I press Control + E,

04:05

the cursor jumps to the end of the line.

04:07

Control + Shift + 6 is another useful key combination.

04:12

This sequence will interrupt the execution of a command

04:15

after the command has already been entered.

04:18

Let's say, for instance,

04:19

I mistyped the command configure

04:24

and press Enter on my keyboard.

04:27

The IOS is trying to translate the letters

04:29

that I typed into an IP address.

04:32

Instead of being stuck in this situation,

04:33

I can simply press Control + Shift + 6

04:37

and the command is aborted.

04:39

Lastly, there may be times when you are working

04:41

on the CLI of a device

04:43

and an event occurs which generates a message

04:46

interrupting the command you are typing.

04:48

This can be very annoying.

04:51

If this occurs, press Control + R on your keyboard

04:55

to return to the prompt where the partial command

04:57

will be displayed allowing you to finish typing.

05:01

This sequence is not currently supported

05:03

in this version of Packet Tracer.

05:05

I'll simulate the use of these hot keys

05:08

by consoling into a physical switch

05:10

and shutting down an interface on the switch

05:12

while I'm in the middle of typing a command.

05:16

I'll press Enter and type "enable"

05:19

to get to Privileged EXEC Mode

05:22

and then I'll go into Global Configuration Mode.

05:26

Let's say I want to enter interface g 0/1.

05:30

I'll start typing the command,

05:33

and now I'll shut down an interface.

05:38

You can see the message displayed across the screen.

05:40

If I simply press Control + R,

05:43

I return to where I left off,

05:46

and I can keep on typing.

05:48

Now that's sweet.

05:51

Using hot keys and shortcuts is a great way

05:53

to save you time when working with the Cisco IOS.

2.3.7 Packet Tracer - Navigate the IOS

In this activity, you will practice skills necessary for navigating the Cisco IOS, including different user access modes, various configuration modes, and common commands used on a regular basis. You will also practice accessing the context-sensitive help by configuring the clock command.

description

Navigate the IOS

file_download

Navigate the IOS

2.3.8 Lab - Navigate the IOS by Using Tera Term for Console Connectivity

Skills Practice Opportunity

You have the opportunity to practice the following skills:

Part 1: Access a Cisco Switch through the Serial Console Port

Part 2: Display and Configure Basic Device Settings

Part 3: (Optional) Access a Cisco Router Using a Mini-USB Console Cable

You can practice these skills using the Packet Tracer or lab equipment, if available.

Packet Tracer - Physical Mode (PTPM)

description

Navigate the IOS Using a Terminal Client for Console Connectivity - Physical Mode

file_download

Navigate the IOS Using a Terminal Client for Console Connectivity - Physical Mode

Lab Equipment

description

Navigate the IOS by Using Tera Term for Console Connectivity

2.4 Basic Device Configuration

2.4.1 Device Names

You have learned a great deal about the Cisco IOS, navigating the IOS, and the command structure. Now, you are ready to configure devices! The first configuration command on any device should be to give it a unique device name or hostname. By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."

The problem is if all switches in a network were left with their default names, it would be difficult to identify a specific device. For instance, how would you know that you are connected to the right device when accessing it remotely using SSH? The hostname provides confirmation that you are connected to the correct device.

The default name should be changed to something more descriptive. By choosing names wisely, it is easier to remember, document, and identify network devices. Here are some important naming guidelines for hosts:

Start with a letter

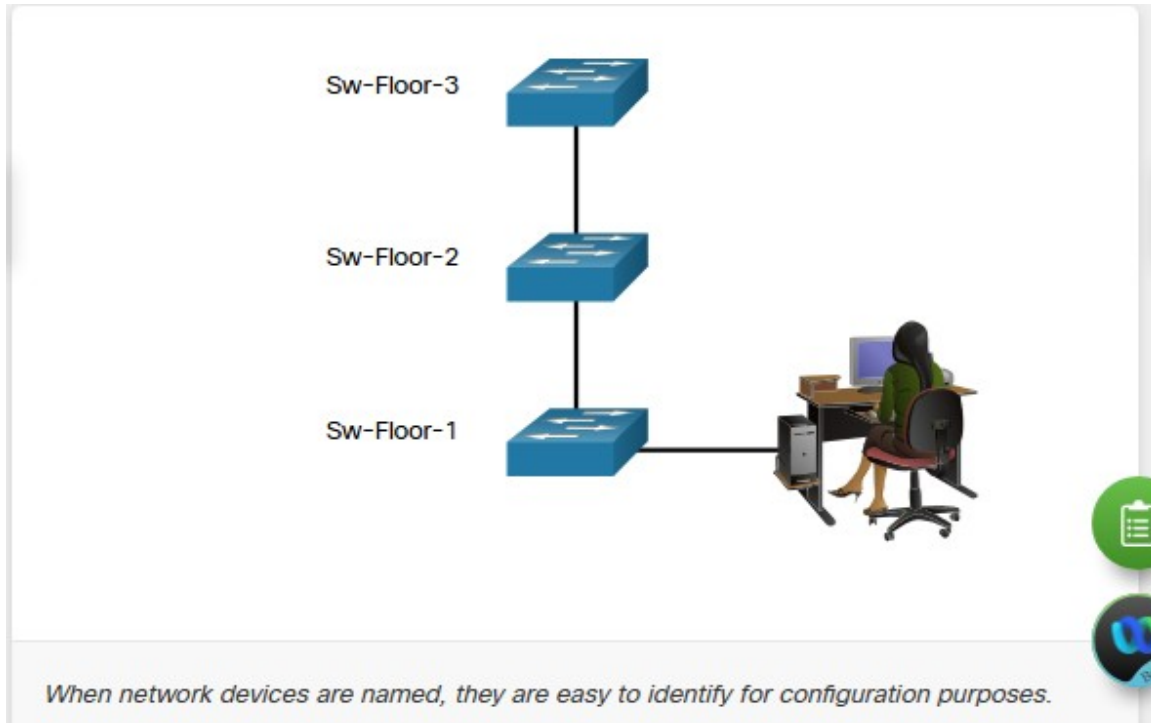
Contain no spaces

End with a letter or digit

Use only letters, digits, and dashes

Be less than 64 characters in length

An organization must choose a naming convention that makes it easy and intuitive to identify a specific device. The hostnames used in the device IOS preserve capitalization and lowercase characters. For example, the figure shows that three switches, spanning three different floors, are interconnected together in a network. The naming convention that was used incorporated the location and the purpose of each device. Network documentation should explain how these names were chosen so additional devices can be named accordingly.



When the naming convention has been identified, the next step is to use the CLI to apply the names to the devices. As shown in the example, from the privileged EXEC mode, access the global configuration mode by entering the configure terminal command. Notice the change in the command prompt.

```
Switch# configure terminal  
Switch(config)# hostname Sw-Floor-1  
Sw-Floor-1(config)#
```

From global configuration mode, enter the command **hostname** followed by the name of the switch and press Enter. Notice the change in the command prompt name.

Note: To return the switch to the default prompt, use the **no hostname** global config command.

Always make sure the documentation is updated each time a device is added or modified. Identify devices in the documentation by their location, purpose, and address.

2.4.2 Password Guidelines

The use of weak or easily guessed passwords continues to be the biggest security concern of organizations. Network devices, including home wireless routers, should always have passwords configured to limit administrative access.

Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device.

All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.

When choosing passwords, use strong passwords that are not easily guessed. There are some key points to consider when choosing passwords:

Use passwords that are more than eight characters in length.

Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.

Avoid using the same password for all devices.

Do not use common words because they are easily guessed.

Use an internet search to find a password generator. Many will allow you to set the length, character set, and other parameters.

Note: Most of the labs in this course use simple passwords such as **cisco** or **class**. These passwords are considered weak and easily guessable and should be avoided in production environments. We only use these passwords for convenience in a classroom setting, or to illustrate configuration examples.

2.4.3 Configure Passwords

When you initially connect to a device, you are in user EXEC mode. This mode is secured using the console.

To secure user EXEC mode access, enter line console configuration mode using **the line console 0** global configuration command, as shown in the example. The zero is used to represent the first (and in most cases the only) console interface. Next, specify the user EXEC mode password using the **password** *password* command. Finally, enable user EXEC access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Console access will now require a password before allowing access to the user EXEC mode.

To have administrator access to all IOS commands including configuring a device, you must gain privileged EXEC mode access. It is the most important access method because it provides complete access to the device.

To secure privileged EXEC access, use **the enable secret** *password* global config command, as shown in the example.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Virtual terminal (VTY) lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

To secure VTY lines, enter line VTY mode using the **line vty 0 15** global config command. Next, specify the VTY password using the **password** *password* command. Lastly, enable VTY access using the **login** command.

An example of securing the VTY lines on a switch is shown.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

2.4.4 Encrypt Passwords

The startup-config and running-config files display most passwords in plaintext. This is a security threat because anyone can discover the passwords if they have access to these files.

To encrypt all plaintext passwords, use the **service password-encryption** global config command as shown in the example.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

The command applies weak encryption to all unencrypted passwords. This encryption applies only to passwords in the configuration file, not to passwords as they are sent over the network. The purpose of this command is to keep unauthorized individuals from viewing passwords in the configuration file.

Use the **show running-config** command to verify that passwords are now encrypted.

```
Sw-Floor-1(config)# end
Sw-Floor-1# show running-config
!
(Output omitted)
!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
password 7 094F471A1A0A
login
line vty 5 15
password 7 094F471A1A0A
login
!
!
end
```

2.4.5 Banner Messages

Although requiring passwords is one way to keep unauthorized personnel out of a network, it is vital to provide a method for declaring that only authorized personnel should attempt to access the device. To do this, add a banner to the device output. Banners can be an important part of the legal process in the event that someone is prosecuted for breaking into a device. Some legal systems do not allow prosecution, or even the monitoring of users, unless a notification is visible.

To create a banner message of the day on a network device, use the **banner motd #** the message of the day **#** global config command. The **"#"** in the command syntax is called the delimiting character. It is entered before and after the message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols such as the **"#"** are often used. After the command is executed, the banner will be displayed on all subsequent attempts to access the device until the banner is removed.

The following example shows the steps to configure the banner on Sw-Floor-1.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only#
```

2.4.6 Video - Secure Administrative Access to a Switch

Click Play in the figure to view a video demonstration of how to secure administrative access to a switch.

Video – Secure Administrative Access to a Switch

This video will cover the following:

- Access the command line to secure the switch
- Secure access to the console port
- Secure virtual terminal access for remote access
- Encrypt passwords on the switch
- Configure the banner message
- Verify security changes

Transcript

Follow along using the transcript.

 Show Transcript

Transcript

16px (
default
)

English

00:06

- [Tutor] When installing a device on a network,

00:08

it's important to secure access to the device

00:11

so only an administrator will be able to access it

00:14

and make changes.

00:15

To do this, we'll need to perform

00:17

some initial configuration settings.

00:19

I'll click on PC1,

00:22

I'll click on the terminal emulation program

00:26

and now you can see, that I have a console connection

00:29

into the switch command line.

00:31

I'll press Enter and this takes me

00:35

to the Command Line Interface.

00:36

As you can see, I'm logged into the switch

00:39

in user exec mode.

00:40

No password was required to access the command line,

00:44

this is a security risk.

00:46

If I type the enable command,

00:48

you can see that I have now entered privilege exec mode

00:52

also without any type of authentication.

00:54

This presents a great security risk since from privilege

00:58

exec mode, I have access to configure the switch.

01:01

The first thing you want to do is secure access

01:03

to both the console connection and to privilege exec mode.

01:07

First, I'll control access to the console connection.

01:10

To do that, I'll get into global configuration mode

01:13

with the config t command and then I'll type in,

01:17

line console zero, to enter line configuration mode.

01:22

I can now put in a password for my console connection

01:25

by typing the command password and a password of cisco.

01:30

For use of this demonstration, I'm using simple passwords,

01:33

but you'll want to use

01:34

strong complex passwords whenever possible.

01:38

I'll type in the login command,

01:40

which will require the password

01:41

prior to entering user exec mode.

01:44

Next, I'll secure access to privilege exec mode.

01:47

To do this, I'll type exit

01:49

to return to global configuration mode.

01:52

Then I'll enter the command enable secret,

01:55

followed by the password class.

01:58

The secret parameter that I used,

02:00

assures me that the password class, will be encrypted

02:03

in the configuration file.

02:04

Let's see if our passwords have been set correctly.

02:07

I'll do a Ctrl + C to get to privilege exec mode

02:10

and then I'll exit the switch.

02:13

Now when I press Enter, I should be prompted for a password

02:16

before establishing a console connection and it does.

02:20

This password should be cisco.

02:22

As I type in the password for security purposes,

02:25

you won't be able to see any characters.

02:27

If I type it in correctly, it should take me

02:30

into user exec mode, and it does,

02:32

and from here, I'll type enable and you can see that,

02:36

now I'm prompted for another password.

02:38

This time, I'll type in class and press Enter

02:41

and you can see now that I'm in privilege exec mode.

02:44

Only those with a knowledge of the correct passwords

02:47

will be able to configure this device.

02:50

Let's take a look at our running configuration file

02:52

up to this point.

02:53

I'll do that by typing in the command, show running-config.

02:59

You can see it the top of the running configuration file

03:02

that the enable secret password,

03:04

has been hashed within the file.

03:06

To see the rest of the configuration,

03:08

I'll press the space bar on my keyboard,

03:11

and I'll go down towards the bottom

03:12

where you can see the configuration for the console line.

03:15

Here, it shows a password of cisco,

03:19

and you can see it in plain text.

03:21

We'll change this a little later.

03:23

Now that I've secured access to the console port,

03:26

I'll also want to secure virtual terminal access

03:28

for remote logins.

03:30

From global configuration mode, I'll type in,

03:35

the command, line vty and then how many lines

03:39

I want to allow remote access to.

03:41

The cisco switch supports 16 simultaneous remote logins

03:45

through virtual terminals.

03:46

To configure all 16, I simply type in zero, a space and 15

03:52

and press Enter and then I'll put in the command,

03:55

password cisco and then login.

03:59

Let's take a look at these passwords

04:01

in our running configuration file.

04:03

I'll do a Ctrl + C to get to privilege exec mode

04:06

and then I'll do a show run,

04:08

which is short for show running config.

04:11

I'll space bar all the way down to the end

04:14

and you can see under the configuration for the console line

04:18

is the vty line configuration.

04:20

The IOS automatically breaks us down into two groups,

04:24

the first five lines zero through four,

04:27

followed by the next 10 lines, five through 15.

04:31

As with the console password, you can see

04:33

that the vty line passwords are also seen in plain text.

04:38

We can add greater security to the switch

04:39

if we can encrypt these passwords, so that they are obscured

04:43

in the configuration file.

04:44

To do this, I'll go back to global configuration mode,

04:48

then I'll enter the command, service password-encryption.

04:55

This command will put a light level of encryption

04:58

on all passwords on the switch.

05:00

To verify that password encryption has been set,

05:03

I'll exit global configuration mode

05:07

and type show run to view the running configuration file.

05:12

If I space bar down to the end, you can now see

05:15

that the console password as well as the vty line password

05:19

has been encrypted.

05:22

Another important initial configuration command

05:25

is setting a banner message.

05:26

This is a message that will be presented to users

05:29

when they log in and serves as a legal warning

05:32

for any would be hackers.

05:34

To do this, I'll go to global configuration mode

05:37

and then I'll type in the command banner motd,

05:41

that stands for message of the day.

05:43

The message that I type will need to be framed

05:46

between two delimiters or characters.

05:48

Just make sure that whatever character you choose

05:50

is not used within the body of your message.

05:53

For instance, I'll use a pound sign for my delimiters

05:57

and then in between, I'll put in the message,

06:00

Authorized access only!

06:04

violators will be prosecuted

06:11

to the full extent of the law!

06:16

And then I'll end it with another pound sign

06:19

and now the banner is set.

06:20

Now let's verify it, I'll do a Ctrl + C,

06:24

and then type exit to leave the switch

06:27

and then I'll press Enter.

06:28

Notice that I'm presented with the banner warning

06:31

I just typed in as well as a request for a password

06:33

just to get access to the console.

06:35

I'll put in the password cisco and press Enter

06:38

and now I'm in user exec mode, and then I'll type,

06:41

the command enable and I'm asked for another password

06:45

to reach privilege exec mode.

06:47

I'll type in class and now I have full access to the switch.

2.4.7 Syntax Checker - Basic Device Configuration

Secure management access to a switch.

Assign a device name.

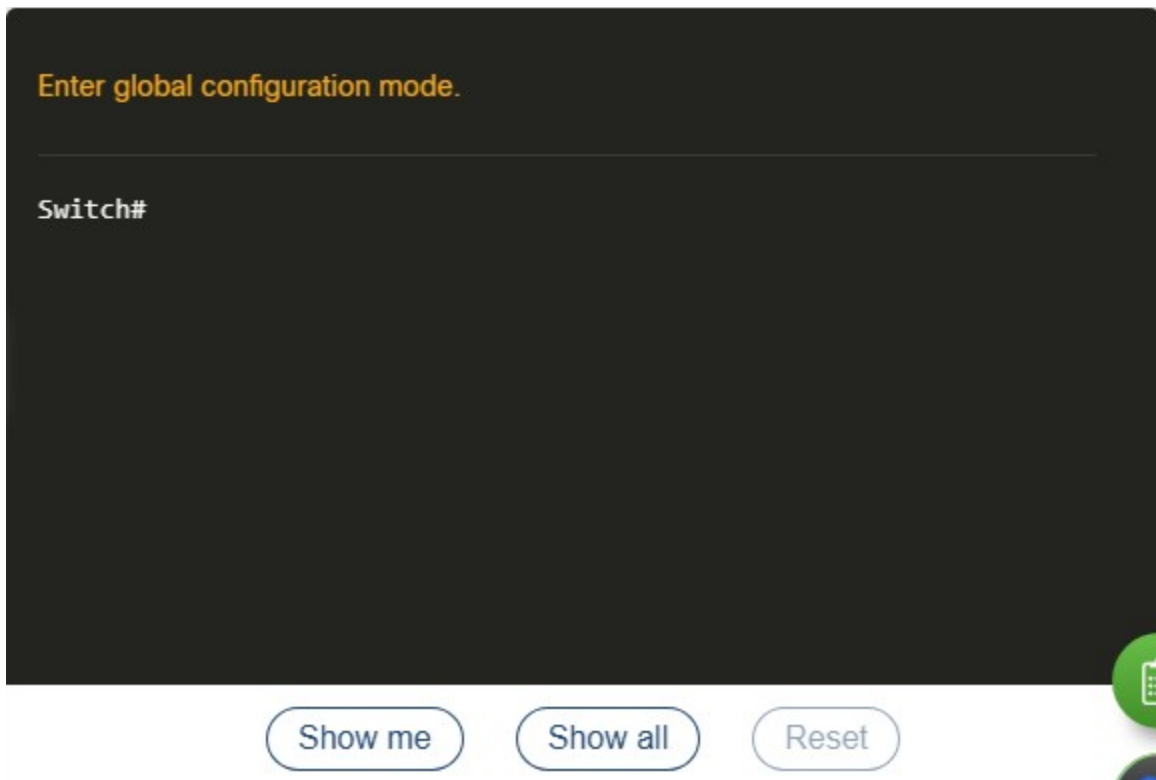
Secure user EXEC mode access.

Secure privileged EXEC mode access.

Secure VTY access.

Encrypt all plaintext passwords.

Display a login banner.



Switch#configure terminal

Name the switch "Sw-Floor-1".

Switch(config)#hostname Sw-Floor-1

Secure user EXEC mode access by entering line console 0, assign the password cisco, enable login, and return to the global configuration mode using exit.

Sw-Floor-1(config)#line console 0

Sw-Floor-1(config-line)#password cisco

Sw-Floor-1(config-line)#login

Sw-Floor-1(config-line)#exit

Secure privileged EXEC mode access using the password class.

Sw-Floor-1(config)#enable secret class

Secure the VTY lines 0 through 15, assign the password cisco, enable login, and return to the global configuration mode using exit.

```
Sw-Floor-1(config)#line vty 0 15
```

```
Sw-Floor-1(config-line)#password cisco
```

```
Sw-Floor-1(config-line)#login
```

```
Sw-Floor-1(config-line)#exit
```

Encrypt all plaintext passwords.

```
Sw-Floor-1(config)#service password-encryption
```

Create a banner message using the “#” symbol as the delimiter. The banner should display exactly: Warning! Authorized access only!

```
Sw-Floor-1(config)#banner motd #Warning! Authorized access only!#
```

You successfully completed the basic requirements to access and secure a device.

2.4.8 Check Your Understanding - Basic Device Configuration

Check your understanding of basic device configuration by choosing the BEST answer to the following questions.

Question 1

What is the command to assign the name “Sw-Floor-2” to a switch?

done

hostname Sw-Floor-2

host name Sw-Floor-2

name Sw-Floor-2

Question 2

How is the privileged EXEC mode access secured on a switch?

enable class

secret class

done

enable secret class

service password-encryption

Question 3

Which command enables password authentication for user EXEC mode access on a switch?

enable secret

done

login

secret

service password-encryption

Question 4

Which command encrypts all plaintext passwords access on a switch?

enable secret

login

secret

done

service password-encryption

Question 5

Which is the command to configure a banner to be displayed when connecting to a switch?

banner \$ Keep out \$

done

banner motd \$ Keep out \$

display \$ Keep out \$

login banner \$ Keep out \$

100%

You've scored 100%.

Congratulations, you have passed the quiz!

You've submitted your answers!

Reset

2.5 Save Configurations

2.5.1 Configuration Files

You now know how to perform basic configuration on a switch, including passwords and banner messages. This topic will show you how to save your configurations.

There are two system files that store the device configuration:

startup-config - This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.

running-config - This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.

The **show running-config** privileged EXEC mode command is used to view the running config. As shown in the example, the command will list the complete configuration currently stored in RAM.

```
Sw-Floor-1# show running-config
Building configuration...
Current configuration : 1351 bytes
!
! Last configuration change at 00:01:20 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Sw-Floor-1
!
(output omitted)
```

To view the startup configuration file, use the **show startup-config** privileged EXEC command.

If power to the device is lost, or if the device is restarted, all configuration changes will be lost unless they have been saved. To save changes made to the running configuration to the startup configuration file, use the copy **running-config startup-config** privileged EXEC mode command.

2.5.2 Alter the Running Configuration

If changes made to the running config do not have the desired effect and the running-config has not yet been saved, you can restore the device to its previous configuration. Remove the changed commands individually, or reload the device using the **reload** privileged EXEC mode command to restore the startup-config.

The downside to using the **reload** command to remove an unsaved running config is the brief amount of time the device will be offline, causing network downtime.

When a reload is initiated, the IOS will detect that the running config has changes that were not saved to the startup configuration. A prompt will appear to ask whether to save the changes. To discard the changes, enter **n** or **no**.

Alternatively, if undesired changes were saved to the startup config, it may be necessary to clear all the configurations. This requires erasing the startup config and restarting the device. The startup config is removed by using the **erase startup-config** privileged EXEC mode command. After the command is issued, the switch will prompt you for confirmation. Press **Enter** to accept.

After removing the startup config from NVRAM, reload the device to remove the current running config file from RAM. On reload, a switch will load the default startup config that originally shipped with the device.

2.5.3 Video - Alter the Running Configuration

Click Play in the figure to view a video demonstration on how to save switch configuration files.

Video – Alter the Running Configuration

This video covers the following:

- Copy the running-config file to the startup-config file
- Show the files in the flash or nvram directory
- Use command shortening
- Erase the startup-config file
- Copy the startup-config file to the running-config file

Transcript

Follow along using the transcript.

 Show Transcript



Transcript

16px (

default

)

English

00:02

- [Male] After you've begun some

00:04

initial configurations on your switch,

00:06

you'll want to know how to save your configuration.

00:10

You can see that I'm using Packet Tracer

00:12

and I have a command line interface to the switch.

00:16

Notice the banner message

00:18

and then I'm being prompted for a password.

00:20

I'll put in the password cisco,

00:23

type enable, password class,

00:26

to get to privileged exec mode.

00:30

I'll type in configure terminal to get to global config mode

00:34

and I'll set the hostname of the switch to S1.

00:38

To save the configuration on the switch,

00:40

I'll go back to privileged exec mode

00:42

by typing exit and pressing enter.

00:45

And then from privileged exec mode,

00:47

I put in the command,

00:48

copy running dash config

00:54

startup dash config.

00:57

This command means copy the running-configuration

01:00

to the startup-configuration file.

01:03

The running-configuration is

01:05

the currently working configuration

01:07

that's running in RAM memory.

01:10

The startup-configuration file is stored in NVRAM memory.

01:15

The difference is that RAM is volatile

01:19

and NVRAM is non-volatile.

01:21

So, if you copied the configuration to NVRAM,

01:24

it will be available when the switch

01:26

is restarted or reloaded.

01:29

So, I'll press Enter

01:30

and you can see that I'm prompted

01:32

for the destination file name.

01:34

The default name is startup dash config

01:36

and you can see it between the brackets.

01:38

I'll press enter to accept the name within the brackets.

01:43

My configuration is now saved.

01:45

I can verify the location of my saved configuration file

01:49

by putting in the command dir for directory.

01:53

I'll put a space and a question mark

01:55

and you can see that there's

01:57

two different types of storage that I have access to.

02:01

Flash memory and NVRAM.

02:04

Both of these are non-volatile.

02:06

The flash memory holds the IOS operating system

02:10

and the NVRAM holds the configuration file.

02:13

I'll put in NVRAM and a colon and press enter

02:18

and you can see there's the startup dash config file.

02:21

Now if I was to reload the switch or incur a power failure,

02:26

my configurations will remain.

02:28

I'll press the arrow keys on my keyboard

02:31

and do an up arrow to go back

02:33

to the command copy running dash config startup dash config.

02:37

There's an easier way of typing this command

02:40

with command shortening.

02:41

Instead of having to type out,

02:43

running dash config and startup dash config,

02:46

I can simply type, copy run start

02:52

and command shortening will finish the command for me.

02:57

If I reload the switch,

02:58

I'll put in the reload command,

03:01

proceed with reload,

03:02

I'll press enter to confirm.

03:04

We'll see that after the switch reloads

03:07

that the hostname will remain S1

03:09

and we should see the same banner message.

03:14

You can see there's the banner message.

03:16

I'm prompted for a password.

03:19

This indicates that the configuration was saved

03:22

and the hostname or device name,

03:24

shows up on the command prompt.

03:26

Also indicating that the configuration

03:28

was successfully saved and reloaded upon startup.

03:33

If I wish to erase the configuration,

03:36

I'll type in enable,

03:37

put in my password to get back to privileged exec mode.

03:40

I can put in the command, erase S-T-A

03:45

I'll press the Tab Key to finish the command

03:48

and the full command is erase startup dash config.

03:52

I'll press enter and I'm giving a warning.

03:55

Do I want to really do this?

03:57

Do I want to continue?

03:59

The default answer is, confirm, so I'll press enter.

04:02

You can see the message output to the screen indicating

04:05

that the NVRAM has been altered or in this case erased.

04:09

I can now reload the switch

04:12

and this time upon reload,

04:14

it should take us directly to the switch command prompt

04:18

without any authentication required or banner message.

04:24

I'll press Enter and you can see that I'm brought directly

04:27

to the switch command prompt.

04:29

The hostname S1 is no longer there nor banner message

04:33

nor line console zero password required.

04:37

Let's say I make some changes to the switch for instance,

04:41

I'll type enable and config T

04:44

to get to global configuration mode

04:47

and I'll change the hostname to MySwitch.

04:53

You can see the device name is now MySwitch.

04:56

I'll exit and save the configuration.

05:03

So the running-configuration has been saved

05:05

to the startup-configuration file.

05:07

Now, let's say I continue

05:09

with some additional configurations.

05:12

I get to global config mode

05:14

and I set a line console zero,

05:19

password to cisco,

05:22

I put in the login command

05:24

and let's say I change the hostname one more time,

05:30

this time to S1.

05:33

Now, I've made these changes.

05:35

Now the current state of the switch

05:37

is that it's running the latest configurations

05:40

in running-configuration.

05:42

That means, the latest configurations

05:43

are running in RAM memory.

05:45

Let's say I'm no longer happy

05:48

with the configurations I've just added to the switch

05:50

and I want to go back to the last saved state.

05:54

The last saved state is where the device name

05:57

was named MySwitch.

05:59

I've changed it now to S1

06:01

but I haven't saved the configuration.

NaN:NaN

I can revert back to the previous saved configuration

06:07

by exiting to privileged exec mode

06:11

and copying in this case,

06:13

not the running-config to the startup-config,

06:15

but the opposite.

06:17

I'll copy the startup-configuration

06:22

to the running-configuration.

06:26

This will load the startup-configuration file into RAM

06:31

and make it the new running-configuration.

06:33

I'll press Enter and I'll accept the default

06:38

and you can see that the switch

06:39

has changed names back to MySwitch.

06:43

The startup-config was loaded into the running-config.

06:47

This does not completely erase the running-config

06:50

but rather the configurations in the startup-config,

06:54

will be merged into the running-config.

06:57

Knowing how to save your configuration

NaN:NaN

and erase a configuration and reload the switch,

07:03

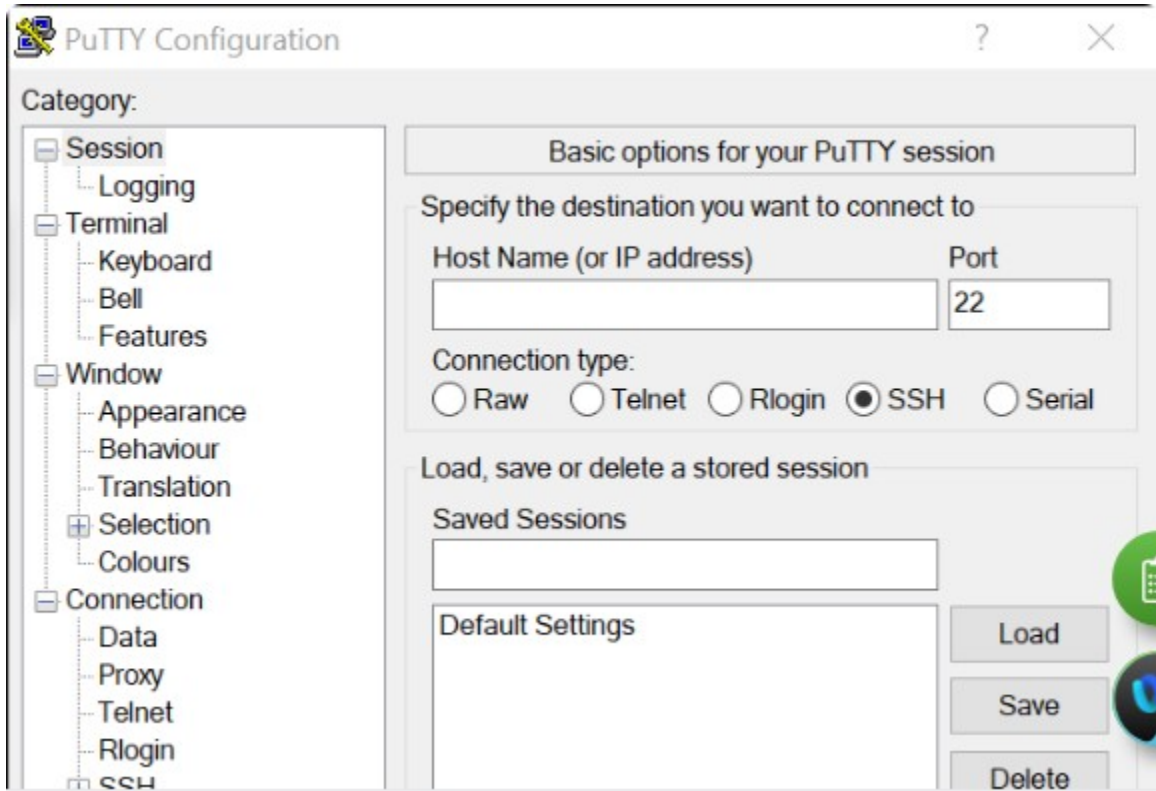
is an important skill to master.

2.5.4 Capture Configuration to a Text File

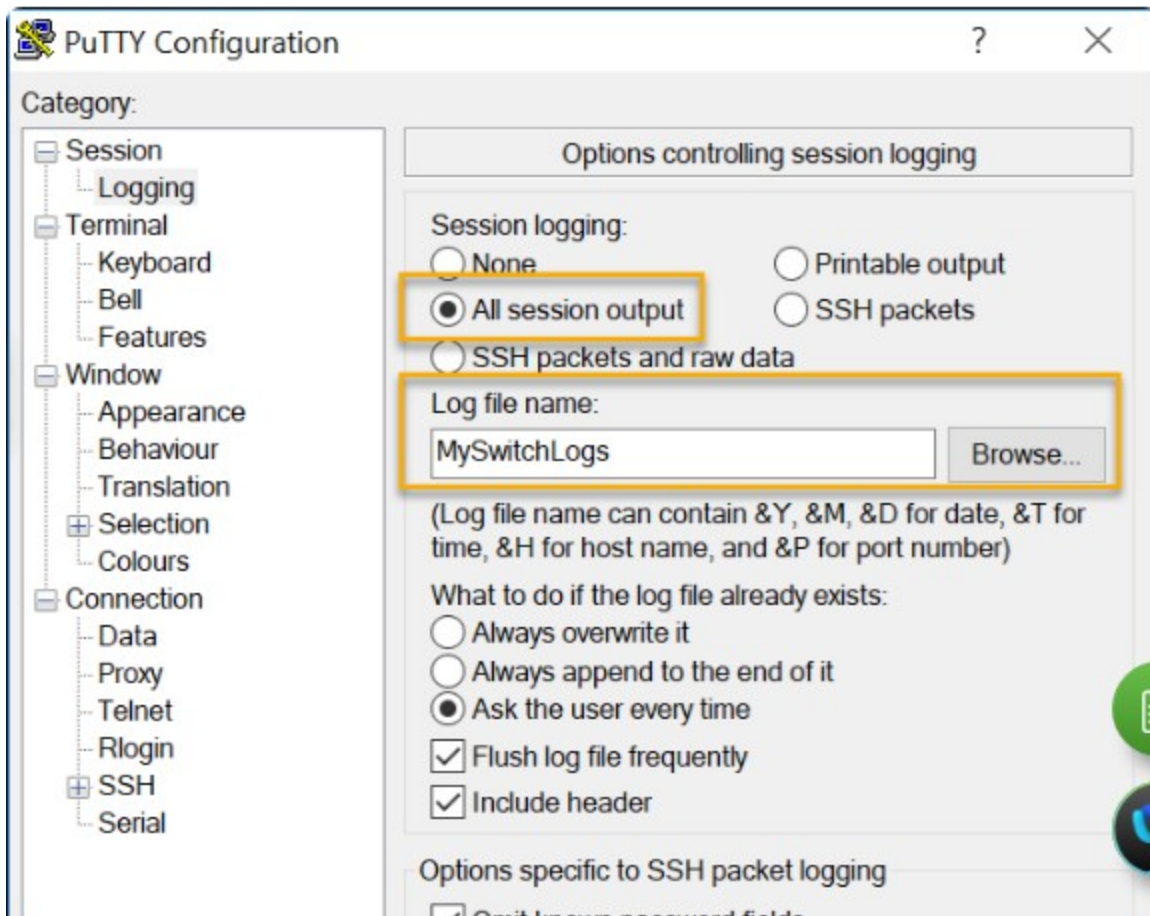
Configuration files can also be saved and archived to a text document. This sequence of steps ensures that a working copy of the configuration file is available for editing or reuse later.

For example, assume that a switch has been configured, and the running config has been saved on the device.

Step 1. Open terminal emulation software, such as PuTTY or Tera Term, that is already connected to a switch.



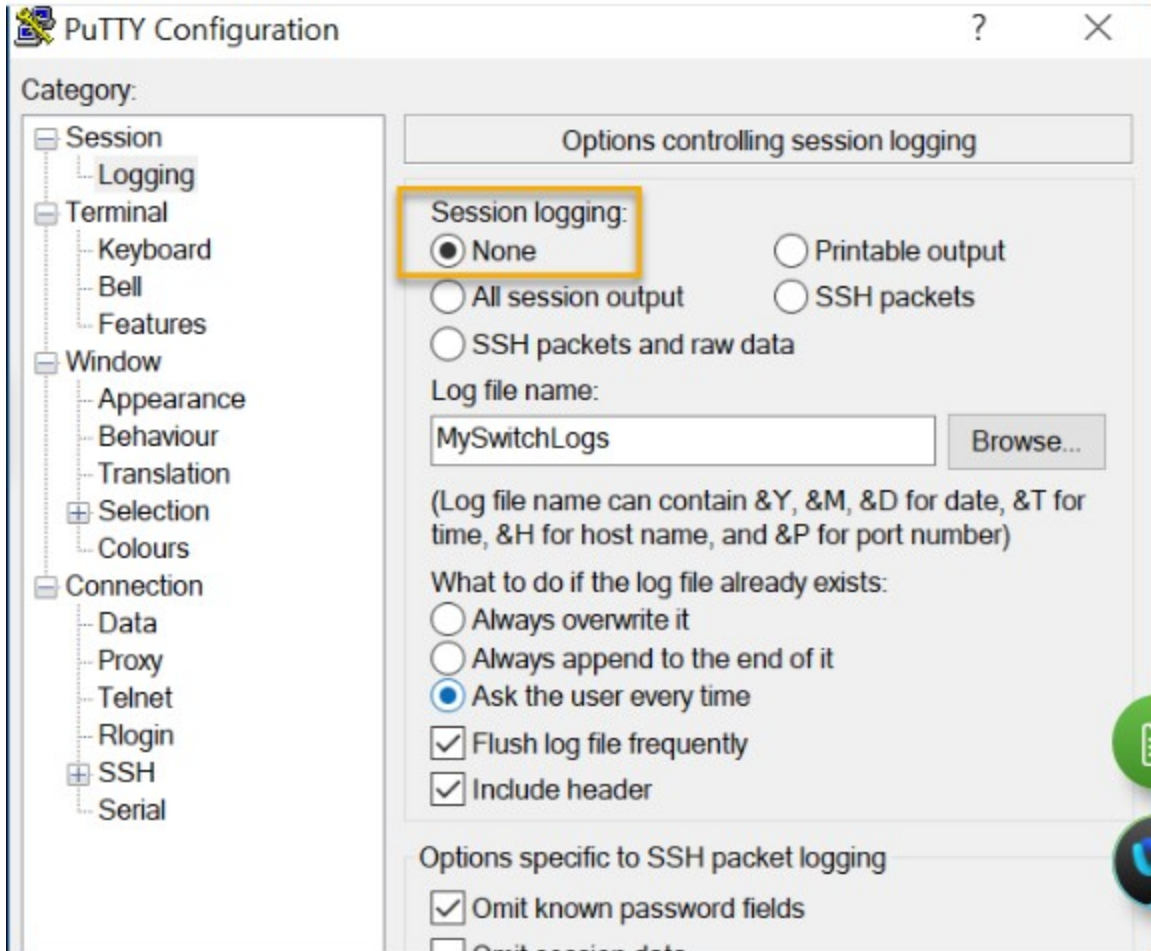
Step 2. Enable logging in the terminal software and assign a name and file location to save the log file. The figure displays that **All session output** will be captured to the file specified (i.e., MySwitchLogs).



Step 3. Execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.

```
Sw-Floor-1# show running-config
Building configuration...
(output omitted)
```

Step 4. Disable logging in the terminal software. The figure shows how to disable logging by choosing the **None** session logging option.



The text file created can be used as a record of how the device is currently implemented. The file could require editing before being used to restore a saved configuration to a device.

To restore a configuration file to a device:

Step 1. Enter global configuration mode on the device.

Step 2. Copy and paste the text file into the terminal window connected to the switch.

The text in the file will be applied as commands in the CLI and become the running configuration on the device. This is a convenient method of manually configuring a device.

2.5.5 Packet Tracer - Configure Initial Switch Settings

In this activity, you will perform basic switch configurations. You will secure access to the CLI and console ports using encrypted and plaintext passwords. You will learn how to configure messages for users logging into the switch. These banners are also used to warn unauthorized users that access is prohibited.

description

Configure Initial Switch Settings

file_download

Configure Initial Switch Settings

2.6 Ports and Addresses

2.6.1 IP Addresses

Congratulations, you have performed a basic device configuration! Of course, the fun is not over yet. If you want your end devices to communicate with each other, you must ensure that each of them has an appropriate IP address and is correctly connected. You will learn about IP addresses, device ports and the media used to connect devices in this topic.

The use of IP addresses is the primary means of enabling devices to locate one another and establish end-to-end communication on the internet. Each end device on a network must be configured with an IP address. Examples of end devices include these:

Computers (work stations, laptops, file servers, web servers)

Network printers

VoIP phones

Security cameras

Smart phones

Mobile handheld devices (such as wireless barcode scanners)

The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255. IPv4 addresses are assigned to individual devices connected to a network.

Note: IP in this course refers to both the IPv4 and IPv6 protocols. IPv6 is the most recent version of IP and is replacing the more common IPv4.

With the IPv4 address, a subnet mask is also necessary. An IPv4 subnet mask is a 32-bit value that differentiates the network portion of the address from the host portion. Coupled with the IPv4 address, the subnet mask determines to which subnet the device is a member.

The example in the figure displays the IPv4 address (192.168.1.10), subnet mask (255.255.255.0), and default gateway (192.168.1.1) assigned to a host. The default gateway address is the IP address of the router that the host will use to access remote networks, including the internet.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:	192 . 168 . 1 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:	.	.	.
-----------------------	---	---	---

IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every four bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. Groups of four hexadecimal digits are separated by a colon (:). IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.

Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☐ Obtain an IPv6 address automatically

☒ Use the following IPv6 address:

IPv6 address: 2001:db8:acad:10::10

Subnet prefix length: 64

Default gateway: fe80::1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

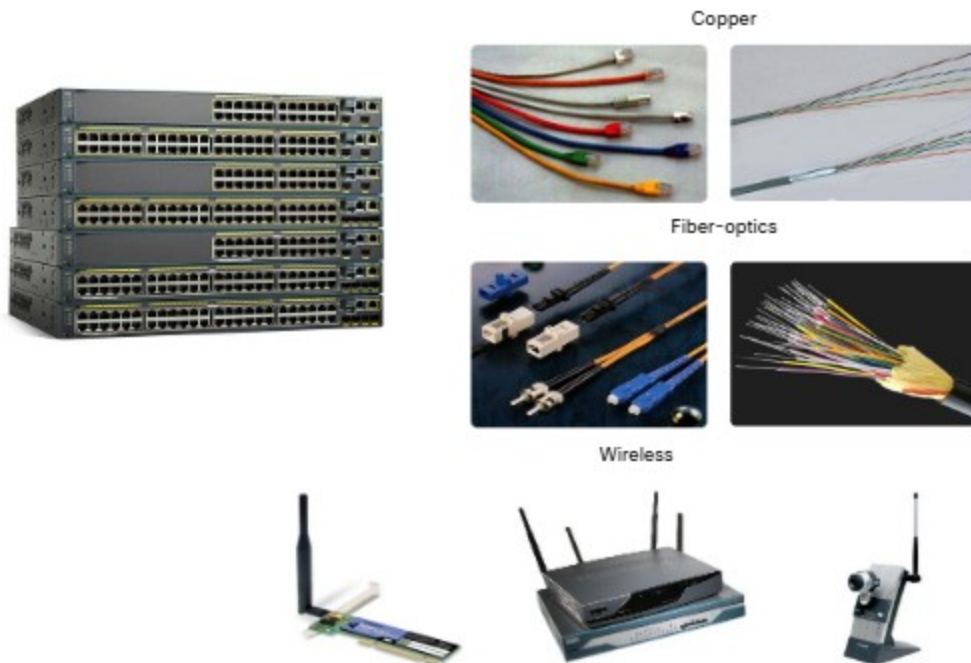
Alternate DNS server:

☐ Validate settings upon exit

Advanced...

2.6.2 Interfaces and Ports

Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them. Each physical interface has specifications, or standards, that define it. A cable connecting to the interface must be designed to match the physical standards of the interface. Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless, as shown in the figure.



Different types of network media have different features and benefits. Not all network media have the same characteristics. Not all media are appropriate for the same purpose. These are some of the differences between various types of media:

- Distance the media can successfully carry a signal
- Environment in which the media is to be installed
- Amount of data and the speed at which it must be transmitted
- Cost of the media and installation

Not only does each link on the internet require a specific network media type, but each link also requires a particular network technology. For example, Ethernet is the most common local-area network (LAN) technology used today. Ethernet ports are found on end-user devices, switch devices, and other networking devices that can physically connect to the network using a cable.

Cisco IOS Layer 2 switches have physical ports for devices to connect. These ports do not support Layer 3 IP addresses. Therefore, switches have one or more switch virtual interfaces (SVIs). These are virtual interfaces because

there is no physical hardware on the device associated with it. An SVI is created in software.

The virtual interface lets you remotely manage a switch over a network using IPv4 and IPv6. Each switch comes with one SVI appearing in the default configuration "out-of-the-box." The default SVI is interface VLAN1.

Note: A Layer 2 switch does not need an IP address. The IP address assigned to the SVI is used to remotely access the switch. An IP address is not necessary for the switch to perform its operations.

2.6.3 Check Your Understanding - Ports and Addresses

Check your understanding of ports and addresses by choosing the BEST answer to the following questions.

Question 1

What is the structure of an IPv4 address called?

Dotted-binary format

done

Dotted-decimal format

Dotted-hexadecimal format

Question 2

How is an IPv4 address represented?

Four binary numbers between 0 and 1 separated by colons.

done

Four decimal numbers between 0 and 255 separated by periods.

Thirty-two hexadecimal numbers separated by colons.

Thirty-two hexadecimal numbers separated by periods.

Question 3

What type of interface has no physical port associated with it?

Console

Ethernet

Serial

done

Switch virtual interface (SVI)

100%

You've scored 100%.

Congratulations, you have passed the quiz!

You've submitted your answers!

Reset

2.7 Configure IP Addressing

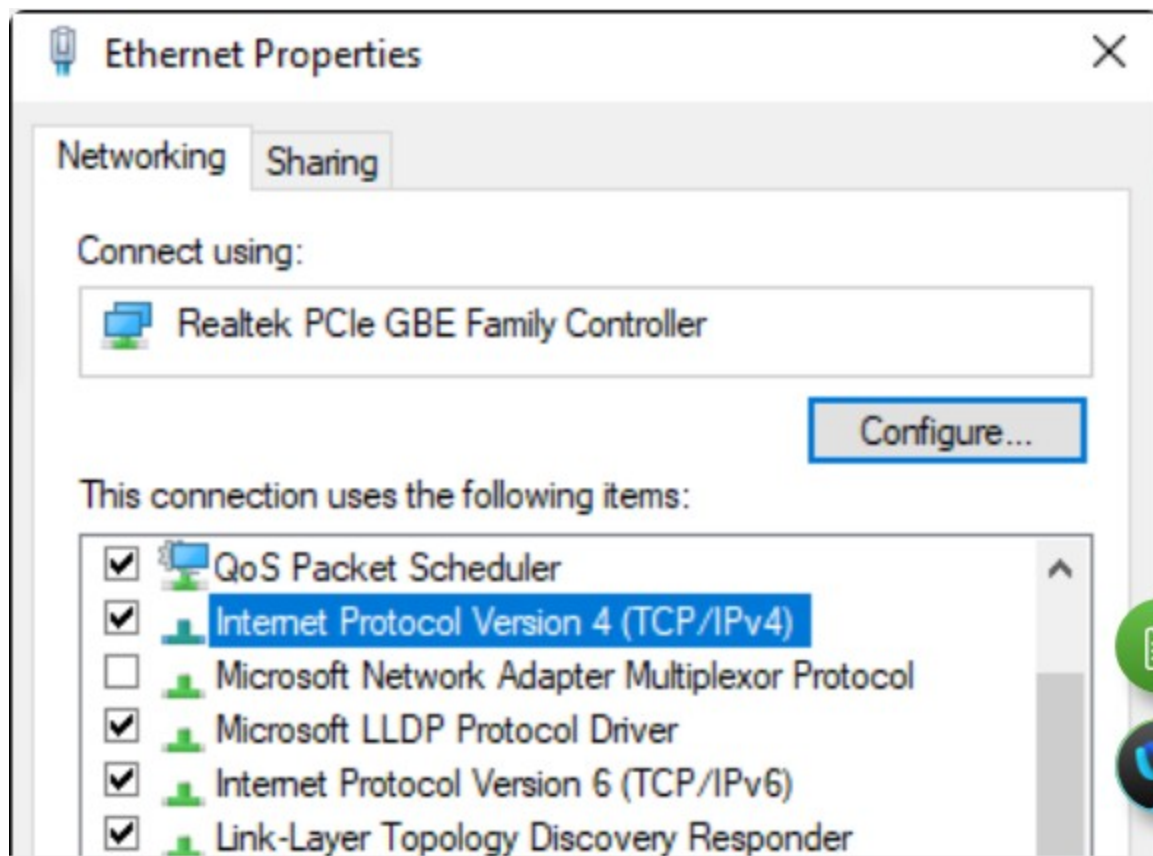
2.7.1 Manual IP Address Configuration for End Devices

Much like you need your friends' telephone numbers to text or call them, end devices in your network need an IP address so that they can communicate

with other devices on your network. In this topic, you will implement basic connectivity by configuring IP addressing on switches and PCs.

IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP).

To manually configure an IPv4 address on a Windows host, open the **Control Panel > Network Sharing Center > Change adapter settings** and choose the adapter. Next right-click and select **Properties** to display the **Local Area Connection** Properties, as shown in the figure.



Highlight Internet Protocol Version 4 (TCP/IPv4) and click **Properties** to open the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, shown in the figure. Configure the IPv4 address and subnet mask information, and default gateway.

Note: IPv6 addressing and configuration options are similar to IPv4.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Note: The DNS server addresses are the IPv4 and IPv6 addresses of the Domain Name System (DNS) servers, which are used to translate IP addresses to domain names, such as www.cisco.com.

2.7.2 Automatic IP Address Configuration for End Devices

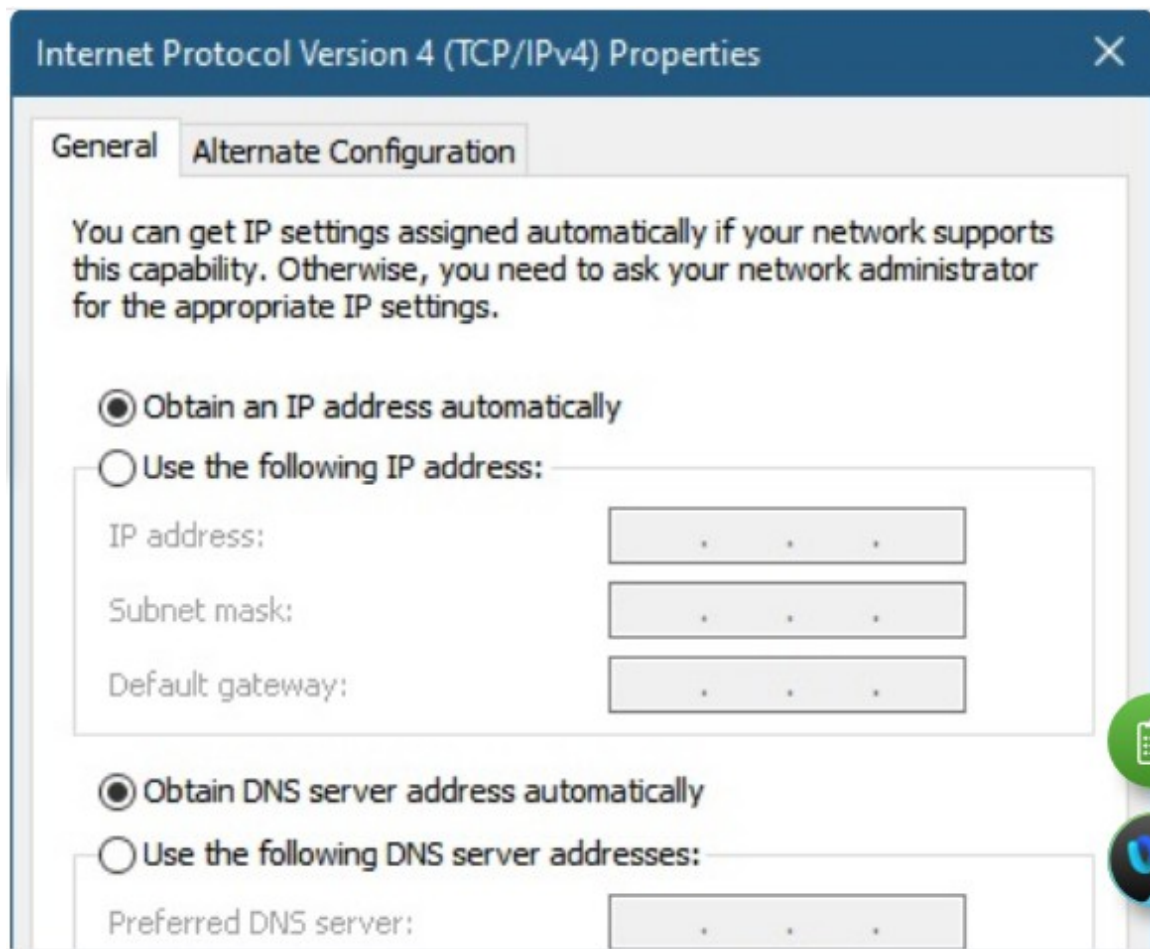
End devices typically default to using DHCP for automatic IPv4 address configuration. DHCP is a technology that is used in almost every network. The best way to understand why DHCP is so popular is by considering all the extra work that would have to take place without it.

In a network, DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled. Imagine the amount of time it would take if every time you connected to the network, you had to manually enter the IPv4 address, the subnet mask, the default gateway, and the DNS server. Multiply that by every user and every device in an organization and you see the

problem. Manual configuration also increases the chance of misconfiguration by duplicating another device's IPv4 address.

As shown in the figure, to configure DHCP on a Windows PC, you only need to select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Your PC will search out a DHCP server and be assigned the address settings necessary to communicate on the network.

Note: IPv6 uses DHCPv6 and SLAAC (**StateLess Address AutoConfiguration**) for dynamic address allocation.



2.7.3 Syntax Checker - Verify Windows PC IP Configuration

It is possible to display the IP configuration settings on a Windows PC by using the ipconfig command at the command prompt. The output will show

the IPv4 address, subnet mask, and gateway information received from the DHCP server.

Enter the command to display the IP configuration on a Windows PC.



Enter the command to display the IP configuration on a Windows PC.

```
C:\>ipconfig
```

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : cisco.com

Link-local IPv6 Address : fe80::b0ef:ca42:af2c:c6c7%16

IPv4 Address. : 192.168.1.10

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.1

You successfully displayed the IP configuration on a Windows PC.

2.7.4 Switch Virtual Interface Configuration

To access the switch remotely, an IP address and a subnet mask must be configured on the SVI. To configure an SVI on a switch, use the **interface vlan 1** global configuration command. Vlan 1 is not an actual physical interface but a virtual one. Next assign an IPv4 address using the **ip address *ip-address subnet-mask*** interface configuration command. Finally, enable the virtual interface using the **no shutdown** interface configuration command.

After these commands are configured, the switch has all the IPv4 elements ready for communication over the network.

Note: Similar to a Windows hosts, switches configured with an IPv4 address will typically also need to have a default gateway assigned. This can be done using the **ip default-gateway *ip-address*** global configuration command. The *ip-address* parameter would be the IPv4 address of the local router on the network, as shown in the example. However, in this module you will only be configuring a network with switches and hosts. Routers will be introduced later.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# interface vlan 1
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
Sw-Floor-1(config-if)# no shutdown
Sw-Floor-1(config-if)# exit
Sw-Floor-1(config)# ip default-gateway 192.168.1.1
```

2.7.5 Syntax Checker - Configure a Switch Virtual Interface

Enter interface configuration mode for VLAN 1.

Switch(config)#

Enter interface configuration mode for VLAN 1.

Switch(config)#interface vlan 1

Configure the IPv4 address as 192.168.1.20 and the subnet mask as 255.255.255.0.

Switch(config-if)#ip address 192.168.1.20 255.255.255.0

Enable the interface.

Switch(config-if)#no shutdown

%LINK-5-CHANGED: Interface Vlan1, changed state to up

You have successfully configured the switch virtual interface for VLAN 1.

2.7.6 Packet Tracer - Implement Basic Connectivity

In this activity, you will first perform basic switch configurations. Then you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use

various show commands to verify configurations and use the ping command to verify basic connectivity between devices.

description

Implement Basic Connectivity

file_download

Implement Basic Connectivity

2.8 Verify Connectivity

2.8.1 Video Activity - Test the Interface Assignment

In the previous topic, you implemented basic connectivity by configuring IP addressing on switches and PCs. Then you verified your configurations and connectivity, because, what is the point of configuring a device if you do not verify that the configuration is working? You will continue this process in this topic. Using the CLI, you will verify the interfaces and the addresses of the switches and routers in your network.

In the same way that you use commands and utilities like **ipconfig** to verify the network configuration of a PC host, you also use commands to verify the interfaces and address settings of intermediary devices like switches and routers.

Click Play in the figure to view a video demonstration of the **show ip interface brief** command. This command is useful for verifying the condition of the switch interfaces.

Follow Along in Packet Tracer

Download the same PKT file that is used in the video. Practice using the ipconfig and **show ip interface brief** commands, as shown in the video.

Video – Test the Interface Assignment

This video will cover the following:

- Connect console cable from PC to switch
- Use terminal emulation program and accept defaults to bring you to command line
- Use enable to enter privileged EXEC mode
- Use global configuration mode and then interface configuration mode to enter no shutdown command

Transcript

Follow along using the transcript.

 Show Transcript

Transcript

16px (
default
)

English

00:03

- [Instructor] In this video, I need to verify

00:05

that the IP addresses 192.168.1.2

00:10

and 192.168.1.3

00:13

have been assigned to switched S1 and S2.

00:17

These IP addresses should have been assigned

00:19

to the default Switched Virtual Interface

00:23

or Interface VLAN1 on both switches.

00:26

In order to verify this, I will first connect

00:29

a console cable from PC-A into Switch S1.

00:33

I click on the console cable, I click on PC-A

00:37

and connect it to the RS-232 serial port

00:41

and then stretch the cable to Switch S1

00:44

and connect it to the console port.

00:47

Now I'll click on PC-A,

00:50

click on the Terminal emulation program,

00:52

and click OK to accept the default configuration setting.

00:56

And this should take me to the command line interface

00:59

on Switch S1.

01:02

From here, I'll type enable to switch

01:04

to Privilege EXEC mode, and then I can issue

01:07

the show ip interface brief command

01:11

to examine the interfaces on Switch S1.

01:15

I will need to press the space bar

01:17

in order to view the full display.

01:19

At the end of the output, you can see Interface VLAN1

01:24

and it has an IP address of 192.168.1.2,

01:29

however if you look in this column, you'll see

01:31

that the state of the interface is administratively down.

01:35

This means that that interface is in a shutdown state.

01:38

You can also see that the line protocol

01:41

of the interface is also down.

01:43

In order to correct that, I first need to go

01:46

into Global Configuration mode.

01:49

Then I'll go into Interface Configuration mode

01:53

for Interface VLAN1, and I will issue

01:56

the no shutdown command, which will activate the interface.

02:00

And you can see that I'm immediately presented

02:02

with a message that indicates that the interface

02:05

has changed its state to up.

02:06

From here I press Enter, Control + C and Enter again

02:10

to return to Privilege EXEC mode.

02:12

And now I can use the Up arrow on my keyboard

02:15

to reissue the show ip interface brief command

02:19

and then verify that now the state of that interface

02:23

is up and up, meaning that it is physically up

02:27

and the line protocol is now up.

02:29

Next, I will verify

NaN:NaN

the Switch Virtual Interface configuration on S2.

02:36

To do that, I will connect a console cable

02:39

from PC-B's serial port

02:42

into the console port of Switch S2.

02:47

Click on PC-B, go to the Desktop tab,

02:51

open the Terminal emulation program,

02:54

accept the default configuration settings,

02:57

and then that should take me

02:59

to the command line interface of Switch S2.

03:06

From here I will enter Privilege EXEC mode

03:10

and then issue the show ip interface brief command

03:16

to examine the interfaces on Switch S2.

03:19

You can see at the end of the output

03:22

we have Interface VLAN1, and at this point,

03:25

it has not yet been assigned an IP address.

03:28

To assign an IP address,

03:30

I will first enter Global Configuration mode

03:34

and then Interface Configuration mode for Interface VLAN1,

03:39

and I'll assign the address by using the ip address command

03:43

and give it the address 192.168.1.3

03:48

followed by its subnet mask.

03:52

In order to activate the interface,

03:54

I will use the no shutdown command, or no shut for short,

03:58

and you can see that the interface

04:00

has changed its state to up.

04:02

From here, I will do Control + C and press Enter

04:06

to return to Privilege EXEC mode and again reissue

04:10

that show ip interface brief command

04:13

to examine the interfaces, press my space bar,

04:18

and at the end of the output, I can see

04:20

that Interface VLAN1 has been assigned

04:23

the IP address 192.168.1.3,

04:28

and the state of the interface is up and up.

download

Test the Interface Assignment

2.8.2 Video Activity - Test End-to-End Connectivity

The **ping** command can be used to test connectivity to another device on the network or a website on the internet.

Click Play in the figure to view a video demonstration using the **ping** command to test connectivity to a switch and to another PC.

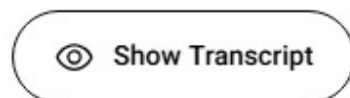
Follow Along in Packet Tracer

Download the same PKT file that is used in the video. Practice using the ping command, as shown in the video.



Transcript

Follow along using the transcript.



Transcript

16px (

default



)

English

00:06

- [Narrator] To test the connections

00:07

between all of the devices,

00:09

as well as the IP address assignments

00:11

on both switches and both PCs,

00:14

I'll use the ping command.

00:15

To do this, I'll click on PC-A,

00:19

click on the Command Prompt,

00:21

and I'll begin by pinging switch S1.

00:27

I will issue the ping 192.168.1.2 command.

00:36

And you can see from the display

00:39

that the first ping request timed out.

00:41

However, I got successful replies for the last three.

00:45

This response is typical

00:47

when you're first testing a connection.

00:49

And the reason for which goes beyond

00:51

the scope of this demonstration.

00:53

If I arrow up and recall that ping command,

00:56

you'll see that now all four echo request packets

01:00

received a reply.

01:02

Next, I'll test connectivity between PC-A and switch S2

01:07

by issuing the ping 192.168.1.3 command.

01:16

Again, you can see that the first request timed out,

01:19

the last three were successful,

01:21

and if I recall the command

01:24

I get four successful echo replies.

01:27

Next I'm going to test connectivity

01:29

between PC-A and PC-B.

01:32

To do that I will ping 192.168.1.11, PC-B's address.

01:43

And you can see that I got responses

01:45

for all four echo requests.

01:47

It's also a good idea to test connectivity

01:50

in the reverse direction.

01:51

To do that, I will click on PC-B,

01:54

click on the Command Prompt,

01:56

and I will issue a ping command

01:59

back to PC-A at address 192.168.1.10.

02:08

And you can see that I get a successful response

02:11

when I ping from PC-B back to PC-A.

02:15

It's always a good idea to test connectivity

02:18

in both directions when working on a real network

02:20

because if you can ping from one device to another

02:23

but not in the reverse direction

02:25

it usually indicates that there is an issue

02:28

with your firewall,

02:29

and by default Windows firewall

02:31

will block ICMP echo requests,

02:34

and needs to be turned off.

file_download

Test End-to-End Connectivity

2.9.4 Module Quiz - Basic Switch and End Device Configuration (Answers)

As a recently hired LAN technician, your network manager has asked you to demonstrate your ability to configure a small LAN. Your tasks include configuring initial settings on two switches using the Cisco IOS and configuring IP address parameters on host devices to provide end-to-end connectivity. You are to use two switches and two hosts/PCs on a cabled and powered network.

Packet Tracer - Skills Integration Challenge Instructions

Packet Tracer - Skills Integration Challenge - PKA

2.9.2 Lab - Basic Switch and End Device Configuration

Skills Practice Opportunity

You have the opportunity to practice the following skills:

Part 1: Set Up the Network Topology

Part 2: Configure PC Hosts

Part 3: Configure and Verify Basic Switch Settings

You can practice these skills using the Packet Tracer or lab equipment, if available.

Packet Tracer - Physical Mode (PTPM)

Basic Switch and End Device Configuration - Physical Mode PDF

Basic Switch and End Device Configuration - Physical Mode pka

Lab Equipment

Basic Switch and End Device Configuration

2.9.3 What did I learn in this module?

All end devices and network devices require an operating system (OS). The user can interact with the shell using a command-line interface (CLI) to use a keyboard to run CLI-based network programs, use a keyboard to enter text and text-based commands, and view output on a monitor.

As a security feature, the Cisco IOS software separates management access into the following two command modes: User EXEC Mode and Privileged EXEC Mode.

Global configuration mode is accessed before other specific configuration modes. From global config mode, the user can enter different subconfiguration modes. Each of these modes allows the configuration of a particular part or function of the IOS device. Two common subconfiguration

modes include: Line Configuration Mode and Interface Configuration Mode. To move in and out of global configuration mode, use the **configure terminal** privileged EXEC mode command. To return to the privileged EXEC mode, enter the **exit** global config mode command.

Each IOS command has a specific format or syntax and can only be executed in the appropriate mode. The general syntax for a command is the command followed by any appropriate keywords and arguments. The IOS has two forms of help available: context-sensitive help and command syntax check.

The first configuration command on any device should be to give it a unique device name or hostname. Network devices should always have passwords configured to limit administrative access. Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device. Configure and encrypt all passwords. Provide a method for declaring that only authorized personnel should attempt to access the device by adding a banner to the device output.

There are two system files that store the device configuration: startup-config and running-config. Running configuration files can be altered if they have not been saved. Configuration files can also be saved and archived to a text document.

IP addresses enable devices to locate one another and establish end-to-end communication on the internet. Each end device on a network must be configured with an IP address. The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255.

IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP). In a network, DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled. To access the switch remotely, an IP address and a subnet mask must be configured on the SVI. To configure an SVI on a switch, use the **interface vlan 1** command in global configuration mode.

In the same way that you use commands and utilities to verify a PC host's network configuration, you also use commands to verify the interfaces and address settings of intermediary devices like switches and routers. The **show ip interface brief** command verifies the condition of the switch interfaces. The **ping** command can be used to test connectivity to another device on the network or a website on the internet.

2.9.4 Module Quiz - Basic Switch and End Device Configuration

Question 1

Which statement is true about the running configuration file in a Cisco IOS device?

It affects the operation of the device immediately when modified.

It is stored in NVRAM.

It should be deleted using the erase running-config command.

It is automatically saved when the router reboots.

Explanation: As soon as configuration commands are entered into a router, they modify the device immediately. Running configuration files can not be deleted nor are they saved automatically.

Question 2

Which two statements are true regarding the user EXEC mode? (Choose two.)

All router commands are available.

Global configuration mode can be accessed by entering the enable command.

The device prompt for this mode ends with the '>' symbol.

Interfaces and routing protocols can be configured.

Only some aspects of the router configuration can be viewed.

Explanation: User EXEC mode limits access to some show and debug commands. It is the first level of user interface encountered when configuring a router and is intended for investigation of certain functions of the device. The User EXEC prompt is identified with the ">" symbol.

Question 3

Which type of access is secured on a Cisco router or switch with the enable secret command?

virtual terminal

privileged EXEC

AUX port

console line

Explanation: The enable secret command secures access to the privileged EXEC mode of a Cisco router or switch.

Question 4

What is the default SVI on a Cisco switch?

VLAN1

VLAN99

VLAN100

VLAN999

Explanation: Layer 2 switches use switch virtual interfaces (SVIs) to provide a means for remote access over IP. The default SVI on a Cisco switch is VLAN1.

Question 5

When a hostname is configured through the Cisco CLI, which three naming conventions are part of the guidelines? (Choose three.)

the hostname should be fewer than 64 characters in length

the hostname should be written in all lower case characters

the hostname should contain no spaces

the hostname should end with a special character

the hostname should begin with a letter

Explanation: A hostname can be configured with upper or lower case characters and should end with a letter or digit, not a special character. A hostname should start with a letter and no space is allowed for a hostname.

Question 6

What is the function of the shell in an OS?

It interacts with the device hardware.

It interfaces between the users and the kernel.

It provides dedicated firewall services.

It provides the intrusion protection services for the device.

Explanation: Most operating systems contain a shell and a kernel. The kernel interacts with the hardware and the shell interfaces between the kernel and the users.

Question 7

A router with a valid operating system contains a configuration file stored in NVRAM. The configuration file has an enable secret password but no console password. When the router boots up, which mode will display?

global configuration mode

setup mode

Privileged EXEC mode

user EXEC mode

Explanation: If a Cisco IOS device has a valid IOS and a valid configuration file, it will boot into user EXEC mode. A password will be required to enter privileged EXEC mode.

Question 8

An administrator has just changed the IP address of an interface on an IOS device. What else must be done in order to apply those changes to the device?

Copy the running configuration to the startup configuration file.

Copy the information in the startup configuration file to the running configuration.

Reload the device and type yes when prompted to save the configuration.

Nothing must be done. Changes to the configuration on an IOS device take effect as soon as the command is typed correctly and the Enter key has been pressed.

Explanation: Changes to router and switch configurations take effect as soon as the command is entered. For this reason, it is very important that changes to live production devices are always carefully planned before being implemented. If commands are entered that render the device unstable or inaccessible, the device may have to be reloaded, resulting in network downtime.

Question 9

Which memory location on a Cisco router or switch will lose all content when the device is restarted?

ROM

flash

NVRAM

RAM

Explanation: RAM is volatile memory and will lose all contents if the router or switch is restarted or shutdown.

Question 10

Why would a technician enter the command `copy startup-config running-config`?

to remove all configurations from the switch

to save an active configuration to NVRAM

to copy an existing configuration into RAM

to make a changed configuration the new startup configuration

Explanation: Usually, changes are made to a running configuration in RAM and copied to NVRAM. However, in this case, the technician wants to copy a previously saved configuration from NVRAM into RAM in order to make changes to it.?

Question 11

Which functionality is provided by DHCP?

automatic assignment of an IP address to each host

remote switch management

translation of IP addresses to domain names

end-to-end connectivity test

Explanation: DHCP provides dynamic and automatic IP address assignment to hosts.

Question 12

Which two functions are provided to users by the context-sensitive help feature of the Cisco IOS CLI? (Choose two.)

providing an error message when a wrong command is submitted

displaying a list of all available commands within the current mode

allowing the user to complete the remainder of an abbreviated command with the TAB key

determining which option, keyword, or argument is available for the entered command

selecting the best command to accomplish a task

Explanation: Context-sensitive help provides the user with a list of commands and the arguments associated with those commands within the current mode of a networking device. A syntax checker provides error checks on submitted commands and the TAB key can be used for command completion if a partial command is entered.

Question 13

Which memory location on a Cisco router or switch stores the startup configuration file?

RAM

ROM

NVRAM

flash

Explanation: The startup configuration file of a Cisco router or switch is stored in NVRAM, which is nonvolatile memory.

Question 14

To what subnet does the IP address 10.1.100.50 belong if a subnet mask of 255.255.0.0 is used?

10.1.0.0

10.0.0.0

10.1.100.32

10.1.100.0

Explanation: The purpose of a subnet mask is to separate the network portion of the address from the host portion of the IP address. The network portion of the IP address is identified by all binary 1s in the subnet mask. Using a subnet mask of 255.255.0.0 identifies the first two octets of the IP address as the network portion.

100%

You have scored 100%.

Congratulations, you have passed the exam.

Reset